**AK+ B.V.**
**Stichting AK+**
**AK+ Special Forces B.V.**
**AK+ Special Forces II B.V.**





**Privacyreglement**

**01-05-2018 – 30-3-2020**

Inhoud

[Doel 4](#_Toc36460739)

[Artikel 1 - Definities 5](#_Toc36460740)

[Artikel 2 - Verantwoordelijkheden en reikwijdte 6](#_Toc36460741)

[2.1 Verantwoordelijkheden 6](#_Toc36460742)

[2.2 Reikwijdte 6](#_Toc36460743)

[Artikel 3 - Informatie en toegang tot de persoonsgegevens 7](#_Toc36460744)

[3.1 Informatie 8](#_Toc36460745)

[3.2 Toegang 9](#_Toc36460746)

[Artikel 4 - Categorie, doel en verwerking persoonsgegevens 10](#_Toc36460747)

[4.1 Personeel 11](#_Toc36460748)

[4.2 Oud-personeelsleden 12](#_Toc36460749)

[4.3 Sollicitanten bij AK+ 13](#_Toc36460750)

[4.4 Medewerkers van klanten 14](#_Toc36460751)

[Artikel 5 - Rechten van betrokkenen 15](#_Toc36460752)

[5.1 Privacyverklaring 16](#_Toc36460753)

[5.2 Recht op informatie 17](#_Toc36460754)

[5.3 Recht op rectificatie en verwijdering 18](#_Toc36460755)

[5.4 Recht op beperking van verwerking 19](#_Toc36460756)

[5.5 Recht op overdraagbaarheid 20](#_Toc36460757)

[5.6 Indiening verzoek 21](#_Toc36460758)

[Artikel 6 - Beveiliging 22](#_Toc36460759)

[6.1 Algemeen 23](#_Toc36460760)

[6.2 Maatregelen  24](#_Toc36460761)

[Artikel 7 - De verwerkingsverantwoordelijke, de (sub)verwerker en de klant 25](#_Toc36460762)

[7.1 Wie 26](#_Toc36460763)

[7.2 Onderlinge verantwoordelijkheden 27](#_Toc36460764)

[Artikel 8 - Inbreuk op de beveiliging / Datalek 28](#_Toc36460765)

[8.1 Inbreuk op de beveiliging 29](#_Toc36460766)

[8.2 Vaststellen + werkwijze datalekken 30](#_Toc36460767)

[Artikel 9 - Klachten 31](#_Toc36460768)

[Artikel 10 – Inwerkingtreding en wijziging 32](#_Toc36460769)

[Bijlage 33](#_Toc36460770)

[Bijlage 1 - Privacyverklaring 34](#_Toc36460771)

[Privacyregels AK+ 34](#_Toc36460772)

[Welke informatie verwerkt AK+? 34](#_Toc36460773)

[Waarom heeft AK+ deze informatie nodig? 34](#_Toc36460774)

[Hoe komt AK+ aan de informatie? 34](#_Toc36460775)

[Geeft AK+ mijn persoonsgegevens ook aan iemand anders? 34](#_Toc36460776)

[Hoelang worden mijn gegevens bewaard? 35](#_Toc36460777)

[Welke rechten heb ik? 35](#_Toc36460778)

[Vragen? Neem contact op met de coördinator informatiebeveiliging 35](#_Toc36460779)

[Bijlage 2 - Formulier melding datalekken 36](#_Toc36460780)

[Bijlage 3 - Formulier registratie datalekken 38](#_Toc36460781)

[Bijlage 4 - Protocol beveiligingsincidenten en datalekken 39](#_Toc36460782)

Doel

Voor de verkoop en levering van diensten door AK+ BV, Stichting AK +, AK Special Forces B.V. en AK Special Forces II B.V. gevestigd te Nijmegen. Deze algemene voorwaarden zijn gedeponeerd bij de Kamer van Koophandel te Nijmegen onder nummer:

* AK+ BV
	+ KVK: 17140403
	+ Vestigingsnr.: 000017897114
* Stichting AK +
	+ KVK: 59801980
	+ Vestigingsnr.: 853649790
* AK Special Forces B.V.
	+ KVK: 65135318
	+ Vestigingsnr.: 000033885079
* AK Special Forces II B.V.
	+ KVK: 68545983
	+ Vestigingsnr.: 000036974501

In het verdere document zullen deze entiteiten onder de noemer AK + worden samengevoegd.

De dienstverlening van AK + is divers waardoor deze voorwaarden bestaan uit een aantal delen. Dit is gedaan om de leesbaarheid van de voorwaarden te bevorderen.

Met het privacyreglement beoogt AK+ ervoor zorg te dragen dat de verwerking van persoonsgegevens plaatsvindt conform de Algemene Verordening Gegevensbescherming (AVG).

Dit houdt onder andere in dat de verwerkingen van persoonsgegevens die plaatsvinden niet zullen leiden tot een hoog risico voor de betrokkenen en wordt voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn. Hiermee is het doel om de persoonlijke levenssfeer van betrokkenen te beschermen tegen verwerkingen, tegen misbruik van die persoonsgegevens, tegen het verwerken van onjuiste gegevens en het waarborgen van de continuïteit van de bedrijfsvoering van onderwijsinstellingen en samenwerkingsverbanden.

AK+ voert passende maatregelen uit en zorgt voor een transparante en verantwoordelijke verwerking van persoonsgegevens.

 Artikel 1 - Definities

Voor de toepassing van dit reglement wordt verstaan onder:

1. *AVG:*Algemene Verordening Gegevensbescherming. Verordening EU 2016/679 van

27 april 2016 betreffende de bescherming van natuurlijke personen in verband met

de verwerking van persoonsgegevens en betreffende het vrije verkeer van die

gegevens en tot intrekking van Richtlijn 95/46/EG*;*

1. *Autoriteit Persoonsgegevens (AP)*: toezichthoudende autoriteit, als bedoeld in

artikel 51 van de AVG;

1. *bestand*: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde

criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

1. *betrokkene*: degene op wie een persoonsgegeven betrekking heeft (personeel, oud-

personeel, sollicitanten bij AK+ en medewerkers van klanten);

1. *derde*: degene, niet zijnde de (sub)verwerker of degene die onder gezag van de

verwerkingsverantwoordelijke werkzaam is, die door de (sub)verwerker is

gemachtigd om persoonsgegevens te verwerken of degene die op grond van wet- en regelgeving bevoegd is om de persoonsgegevens te ontvangen;

1. *klant/onderwijsinstelling*: schoolbestuur en/of samenwerkingsverbanden en/of andere opdrachtgever waarvoor AK+ diensten verricht en tegelijkertijd de verwerkings- verantwoordelijke ten aanzien van de persoonsgegevens van medewerkers van de klant;
2. *personeelsnummer*: eenduidig nummer dat wordt gebruikt ten behoeve van

efficiënte verwerking van persoonsgegevens;

1. *personeel*:
2. de bij de AK+ werkzame directeur en medewerkers op basis van een

arbeidsovereenkomst;

1. de onder a bedoelde medewerker die zonder arbeidsovereenkomst is

tewerkgesteld bij of ingeleend door de AK+;

i. *persoonsgegevens*: alle informatie over een geïdentificeerde of identificeerbare

natuurlijke persoon (‘de betrokkene’);

j.*toestemming van betrokkene*: elke vrije, specifieke, geïnformeerde

ondubbelzinnige wilsuiting door middel van de privacyverklaring of een ondubbelzinnig actieve handeling;

k.*verwerking van persoonsgegevens*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen,

 gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen of vernietigen van gegevens;

l.*verwerkingsverantwoordelijke*: AK+ ten aanzien van de persoonsgegevens van het (eigen) personeel;

m.*(sub)verwerker*: AK+ in relatie tot de klant/onderwijsinstelling met wie zij een

  dienstverleningsovereenkomst is overeengekomen en ten behoeve daarvan

persoonsgegevens verwerkt, zonder dat zij rechtstreeks aan het gezag van die klant is onderworpen. Daarnaast de derde in relatie tot AK+ met wie zij een

  overeenkomst sluit ten behoeve van de verwerking van persoonsgegevens.

n.  *AK+:*waar in het reglement wordt gesproken over AK+ worden alle verschillende

entiteiten bedoeld, dat wil zeggen AK+ B.V., Stichting AK+, AK+ Special Forces  B.V. en AK+ Special Forces II B.V..

# Artikel 2 - Verantwoordelijkheden en reikwijdte

## 2.1 Verantwoordelijkheden

AK+ ondersteunt klant(en)/onderwijsinstelling(en) in haar bedrijfsvoering. Hierbij worden persoonsgegevens verwerkt. AK+ is een (sub)verwerker die uitvoering geeft aan de

opdracht van een onderwijsinstelling. In die hoedanigheid draagt AK+ als (sub)verwerker

van persoonsgegevens niettemin verantwoordelijkheid om de gegevensverwerking van

betrokkenen conform de AVG te laten plaatsvinden. Hiervoor is AK+:

* verantwoordelijk voor de naleving van de bepalingen in dit reglement en het binnen

de organisatie vastgestelde beleid;

* Treft maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij

worden verwerkt, juist en nauwkeurig zijn;

* Draagt er zorg voor dat personeel kennis heeft van zijn verantwoordelijkheden en

verplichtingen bij de verwerking van persoonsgegevens;

* Beschikt over een register van verwerkingsactiviteiten voor de gegevensverwerkingen die hij voor de verschillende categorieën van betrokkene uitvoert.

## 2.2 Reikwijdte

Dit reglement stelt regels over de verwerking van persoonsgegevens van personeel, oud-personeel en sollicitanten van AK+ en de werknemers van klanten. Dit reglement is van toepassing op alle persoonsgegevens van betrokkenen die door AK+ worden verwerkt.

Dit reglement geeft uitleg over het gebruik van persoonsgegevens en dient bewustwording te creëren.

Artikel 3 - Informatie en toegang tot de persoonsgegevens

3.1 Informatie

AK+ informeert haar personeel voorafgaand aan de verzameling van de persoonsgegevens welke persoonsgegevens worden verwerkt en met welk doel dat gebeurt of wat de grondslag hiervan is. Daarnaast registreert AK+ met wie de gegevens worden gedeeld (in- en extern) en hoe lang en waar de gegevens worden bewaard. Betrokkene wordt door middel van een privacyverklaring op de hoogte gesteld van de verwerking van zijn/haar persoonsgegevens. Aan betrokkene wordt tegelijkertijd gevraagd zijn/haar toestemming hiervoor te verlenen en wordt betrokkene gewezen op zijn/haar rechten op grond van de AVG *(bijlage 1 - Privacyverklaring)*. De rechten die betrokkene heeft zijn uitgewerkt in artikel 5 van dit Privacyreglement.

3.2 Toegang

Eenieder die betrokken is bij de uitvoering van dit reglement en daarbij de toegang krijgt tot persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan en tekent de geheimhoudingsverklaring. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

AK+ hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens. Hierdoor heeft personeel geen toegang tot meer persoonsgegevens dan strikt noodzakelijk is voor de uitoefening van hun functie.

Artikel 4 - Categorie, doel en verwerking persoonsgegevens

Hieronder vindt u per categorie een opsomming van welke persoonsgegevens - en met welk doel - worden verwerkt.

4.1 Personeel

**Doel**

1. Het aangaan van een arbeidsovereenkomst;
2. Het vaststellen van salarisafspraken en arbeidsvoorwaarden;
3. De salarisuitbetaling met het oog op afdracht belastingen en premies;
4. De uitvoering arbeidsvoorwaarde(n);
5. Het innen van vorderingen;
6. Het verlenen van ontslag;
7. De tewerkstelling bij een ander onderdeel van AK+ (bijv. Special Forces);
8. Het leidinggeven aan betrokkene;
9. Het verstrekken van bedrijfsmedische zorg en het nakomen van re-integratieverplichtingen;
10. Het toegang verlenen tot het bedrijfsnetwerk en financiële- en salarisverwerkingssytemen;
11. Het regelen en de controle op aanspraak op uitkeringen in verband met beëindiging dienstverband;
12. Het behandelen van geschillen en het uitbrengen van advies met betrekking tot rechtspositionele zaken en geschillen;
13. De behandeling van personeelszaken anders dan genoemd onder a. t/m l;
14. Het organiseren van de bedrijfsvoering;
15. Het laten uitoefenen van een accountantscontrole;
16. De beveiliging van en toezicht op personen, zaken en gebouwen;
17. Commerciële doeleinden.

**Verwerking persoonsgegevens**

1. De NAW- en communicatiegegevens;
2. Het BSN-nummer;
3. Een kopie ID-bewijs / paspoort;
4. Het personeelsnummer;
5. De nationaliteit / geboorteplaats;
6. Een Verklaring Omtrent Gedrag (VOG);
7. De gevolgde en te volgen opleidingen/cursussen/stages;
8. Die relevant zijn gelet op de arbeidsvoorwaarden;
9. Salaris / vergoedingen / beloningen (in natura);
10. Belasting / premies;
11. Voormalige functie(s) / dienstverbanden;
12. Administratie aan- en afwezigheid;
13. De gegevens in het belang van de arbeidsomstandigheden en veiligheid;
14. Betreffende gezinsleden van betrokkene, die noodzakelijk zijn voor effectuering van de arbeidsvoorwaarden;
15. Over de functie-oefening / personeelsbeoordeling / loopbaanbegeleiding;
16. Gegevens voor zover van belang voor de inrichting van de organisatie en/of van belang in de uitoefening van de functie;
17. Inloggegevens tot het bedrijfsnetwerk en financiële- en salarisverwerkingssystemen;
18. (Pas)foto’s van het personeel en camerabeelden (met of zonder geluid) van de ingang van de organisatie
19. De gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt;
20. Andere dan onder a t/m s. bedoelde gegevens.

4.2 Oud-personeelsleden

**Doel**

1. Onderhouden van contacten met oud-personeelsleden;
2. Verzenden van informatie aan oud-personeelsleden;
3. Verwerken van de aanmeldingen van oud-personeelsleden voor activiteiten en bijeenkomsten;
4. Het doen uitoefenen van accountantscontrole.

**Verwerking persoonsgegevens**

1. NAW- en communicatiegegevens;
2. Gegevens betreffende de functie waarin en de periode gedurende welke het oud-personeelslid voor AK+ werkzaam is geweest;
3. Een administratiecode dat geen andere informatie bevat dan bedoeld onder a. en b.

4.3 Sollicitanten bij AK+

**Doel**

1. Beoordeling van de geschiktheid van betrokkene;
2. De beoordeling van de geschiktheid van betrokkene voor een functie die in de nabije toekomst vacant kan komen;
3. De afhandeling van de door de sollicitant gemaakte onkosten;
4. Beveiliging van en toezicht op personen, zaken en gebouwen;
5. De uitvoering of toepassing van wetgeving.

**Verwerking persoonsgegevens**

1. NAW- en communicatiegegevens;
2. Nationaliteit en geboorteplaats;
3. Gevolgde en te volgen opleidingen/cursussen/stages;
4. Gegevens betreffende de functie waarnaar is gesolliciteerd;
5. Gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, (alsmede de beëindiging ervan);
6. Gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
7. Camerabeelden met of zonder geluid van de ingang van de organisatie;
8. Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
9. Andere gegevens die door of na toestemming van de betrokkene zijn verstrekt;
10. Andere dan onder a. tot en met i. bedoelde gegevens.

4.4 Medewerkers van klanten

**Doel**

1. het aangaan van een arbeidsovereenkomst;
2. Het vaststellen van salarisafspraken en arbeidsvoorwaarden;
3. De salarisuitbetaling met het oog op afdracht belastingen en premies;
4. De uitvoering arbeidsvoorwaarde(n);
5. Het innen van vorderingen;
6. Het verlenen van ontslag;
7. De tewerkstelling bij een ander onderdeel van de groep;
8. Het verstrekken van bedrijfsmedische zorg en het nakomen van re-integratieverplichtingen;
9. Het toegang verlenen tot het salarisverwerkingssytemen;
10. Het regelen en controleren van de aanspraak op uitkeringen in verband met de beëindiging van dienstverband;
11. Het afwikkelen van geschillen;
12. De organisatie van - of het geven van het - onderwijs;
13. Het voldoen aan - en handhaven van - de bekwaamheidseisen en de borging van een ordentelijk systeem en van goede zeden in het kader van (het recht op) kwalitatief goed onderwijs (Wijzigingsbesluit  van 7 juni 2017 tot wijziging van het Besluit informatievoorziening WPO/WEC, Besluit informatievoorziening WVO en het Uitvoeringsbesluit WEB);
14. Het laten uitoefenen van een accountantscontrole en/of het vaststellen van aanspraken met betrekking tot bekostiging;
15. Persoonsgegeven ten behoeve van het lerarenregister en het registervoorportaal;
16. De verwerking van gegevens ten behoeve van de bedrijfsvoering, anders dan genoemd onder a. tot en met o.

**Verwerking persoonsgegevens**

1. De NAW- en communicatiegegevens;
2. Het BSN-nummer;
3. Een kopie ID-bewijs / paspoort;
4. Het personeelsnummer;
5. De nationaliteit / geboorteplaats;
6. Een Verklaring Omtrent Gedrag (VOG);
7. De gevolgde en te volgen opleidingen/cursussen/stages;
8. Die relevant zijn gelet op de arbeidsvoorwaarden;
9. Salaris / vergoedingen / beloningen (in natura);
10. Belasting / premies;
11. Voormalige functie(s) / dienstverbanden;
12. Administratie aan- en afwezigheid;
13. Betreffende gezinsleden van betrokkene, die noodzakelijk zijn voor effectuering van de arbeidsvoorwaarden;
14. Inloggegevens salarisverwerkingssysteem;
15. Andere dan de onder a. tot en met n. bedoelde gegevens waarvan de verwerking wordt vereist.

Artikel 5 - Rechten van betrokkenen

5.1 Privacyverklaring

AK+ beschikt over een privacyverklaring *(Bijlage 1 - Privacyverklaring)*, waarin betrokkenen in duidelijke, begrijpelijke en gemakkelijke toegankelijke vorm worden geïnformeerd over de gegevens die van hem worden verwerkt, de wijze waarop en de redenen waarom dit gebeurt.

5.2 Recht op informatie

Betrokkenen van wie persoonsgegevens worden verwerkt hebben het recht van inzage in - en recht op een kopie van - de over hen opgenomen gegevens en van de volgende informatie over:

1. De verwerkingsdoeleinden en de rechtsgrond voor de verwerking;
2. De betrokken categorieën van persoonsgegevens;
3. De ontvangers en/of categorieën van ontvangers aan wie de persoonsgegevens
zullen worden verstrekt;
4. De periode gedurende welke de persoonsgegevens naar verwachting zullen
worden opgeslagen;
5. De herkomst van de verwerkte gegevens indien deze niet van betrokkene
afkomstig zijn;
6. Het bestaan van geautomatiseerde besluitvorming.

5.3 Recht op rectificatie en verwijdering

Betrokkenen hebben het recht op rectificatie van onjuiste persoonsgegevens en het recht op verwijdering van gegevens in de volgende situaties:

1. De persoonsgegevens zijn niet meer nodig;
2. de betrokkene trekt de toestemming waarop de verwerking berust in en er
geen andere rechtsgrond voor die verwerking is;
3. de betrokkene bezwaar maakt tegen de verwerking en er geen prevalerende
dwingende vormen voor verwerking zijn;
4. de persoonsgegevens onrechtmatig zijn verwerkt;
5. een wettelijke verplichting om de persoonsgegevens te wissen.

5.4 Recht op beperking van verwerking

Betrokkene heeft op grond van de AVG in nader bepaalde situaties recht op beperking van de verwerking van zijn gegevens. AK+ verwerkt de persoonsgegevens slecht met toestemming van betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter uitvoering van de dienstverleningsovereenkomst met de klant of ter bescherming van de rechten van een ander natuurlijk persoon of rechtspersoon of om gewichtige redenen van algemeen belang.

5.5 Recht op overdraagbaarheid

Betrokkene heeft het recht om de hem betreffende persoonsgegevens die hij zelf aan AK+ heeft verstrekt in een gestructureerde en digitaal leesbare vorm te verkrijgen. Daarnaast heeft hij het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen in de gevallen dat persoonsgegevens door hem op basis van verleende toestemming zijn verstrekt of op basis van een overeenkomst en de verwerking geautomatiseerd plaatsvindt.

Het recht geldt niet voor verwerkingen die noodzakelijk zijn voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan verwerkingsverantwoordelijke of de klant is verleend.

5.6 Indiening verzoek

Betrokkene kan een verzoek indienen bij AK+ en zijn verzoek richten aan de coördinator informatiebeveiliging.

Als een verzoek van betrokkene kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter kan AK+ een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verzoek gepaard gaat of weigeren gevolg te geven aan het verzoek.

AK+ verstrekt aan betrokkene, als verwerkingsverantwoordelijke zijnde, binnen één maand na ontvangst van het verzoek een schriftelijke beslissing. Afhankelijk van de complexiteit van het verzoek of de hoeveelheid verzoeken kan die termijn indien noodzakelijk met twee maanden worden verlengd. AK+ stelt betrokkene binnen een maand in kennis van een dergelijke verlenging.

Indien AK+ geen gevolg wenst te geven aan een verzoek als bedoeld in artikel 5 doet hij hiervan - gemotiveerd - schriftelijk mededeling aan betrokkene.

De betrokkene die zich niet kan verenigen met de afwijzing van zijn verzoek als bedoeld in dit artikel kan zich wenden tot de AP benaderen met een verzoek tot bemiddeling.

Artikel 6 - Beveiliging

6.1 Algemeen

AK+ heeft passende technische en organisatorische maatregelen genomen om persoonsgegevens doeltreffend te beveiligen en beveiligd te houden tegen verlies of een vorm van onrechtmatig gebruik en/of verwerking. Hierbij wordt rekening gehouden met technologische ontwikkelingen, de kosten van de tenuitvoerlegging van deze maatregel en de aard van de te beschermen persoonsgegevens.

6.2 Maatregelen

Met betrekking tot persoonsgegevens neemt AK+ in ieder geval de volgende maatregelen in aanmerking:

1. Er wordt een autorisatiebeleid gehanteerd om te bepalen wie toegang moet
hebben tot welke gegevens. Op grond van deze systematiek heeft personeel
geen toegang tot meer persoonsgegevens dan strikt noodzakelijk is voor de
uitoefening van de functie.
2. AK+ houdt een register (PSA-overzicht) bij van alle categorieën van
verwerkingsactiviteiten.
3. AK+ heeft dit privacyreglement opgesteld, zodat het personeel zich
bewust is van - en op de hoogte is - hoe zij moet omspringen met (het
verwerken) persoonsgegevens.
4. AK+ heeft een coördinator informatiebeveiliging (intern) om risico’s
omtrent de verwerking van persoonsgegevens te inventariseren,
beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen
te treffen die zien op de naleving van het informatiebeveiligingsbeleid.
5. Datalekken worden gedocumenteerd en benut voor
optimalisatie van het informatiebeveiligingsbeleid (werkplekbeheersysteem).
6. AK+ heeft een proces ingericht voor de communicatie over
beveiligingsincidenten en datalekken (*bijlage 2 - Formulier melding datalekken,*
*bijlage 3 - Formulier registratie datalekken* en *bijlage 4 - Protocol*
*beveiligingsincidenten en datalekken).*
7. Het personeel ondertekent een geheimhoudingsverklaring (zie artikel 3.2).
8. AK+ stimuleert het bewustzijn, opleiding en training ten aanzien van
informatiebeveiliging.
9. Persoonsgegevens worden uitsluitend verwerkt in een gesloten en fysiek
beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
10. Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij
maatregelen zijn genomen om de apparatuur fysiek te beveiligen.
11. De ondersteunende software is extern (webbased) opgeslagen. De
betreffende partij(en) garanderen dagelijkse back-ups. Deze back-ups worden
vertrouwelijk behandeld en bewaard.
12. De locatie(s) waar gegevens worden verwerkt worden periodiek getest,
onderhouden en periodiek onderhouden op beveiligingsrisico’s
(werkplekbeheersysteem).
13. De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt
beveiligd. Verkeersstromen worden gescheiden en er zijn maatregelen
geïmplementeerd tegen misbruik en aanvallen (Firewall Kaspersky).
14. Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd
op basis van patchmanagement (werkplekbeheersysteem).
15. Niet (meer) gebruikte informatie wordt met inachtneming van de
bewaartermijn verwijderd.
16. Binnen AK+ wordt periodiek het beveiligingsbeleid in interne processen en
kwetsbaarheden besproken.
17. AK+ actualiseert deze informatie voortdurend en informeert haar werknemers
over wijzigingen in de getroffen maatregelen om persoonsgegevens te
beschermen tegen misbruik.

Artikel 7 - De verwerkingsverantwoordelijke, de (sub)verwerker en de klant

7.1 Wie

Ten aanzien van haar eigen personeel, oud-personeelsleden en ten aanzien van sollicitanten van AK+, is AK+ de verwerkingsverantwoordelijke. Ten aanzien van medewerkers van de klant/onderwijsinstelling blijft de klant/onderwijsinstelling verwerkingsverantwoordelijke.

De (sub)verwerker is AK+ in relatie tot de klant/onderwijsinstelling met wie een verwerkersovereenkomst is gesloten. De (sub)verwerker is ook degene die op basis van een overeenkomst voor of namens AK+ gegevens verwerkt. De (sub)verwerker verwerkt persoonsgegevens op de wijze zoals overeengekomen in een verwerkersovereenkomst.

De klant/onderwijsinstelling, is het schoolbestuur of het samenwerkingsverband of andere opdrachtgever met wie AK+ een dienstverleningsovereenkomst heeft gesloten.

7.2 Onderlinge verantwoordelijkheden

De verwerkingsverantwoordelijke heeft en houdt zeggenschap over het doel en de middelen van de verwerking van de persoonsgegevens.

De (sub)verwerker is verantwoordelijk voor het juiste gebruik van de nodige voorzieningen om de bescherming van de persoonlijke levenssfeer van de personen van wie gegevens worden verwerkt, in voldoende mate te waarborgen, zoals is opgenomen in de verwerkersovereenkomst.

De coördinator informatiebeveiliging ziet erop toe dat de bedoelde voorzieningen worden getroffen en in acht worden genomen.

Artikel 8 - Inbreuk op de beveiliging / Datalek

8.1 Inbreuk op de beveiliging

Indien er binnen de organisatie van AK+, of indien van toepassing bij een door AK+ ingeschakelde (sub)verwerker, een inbreuk op de beveiliging plaatsvindt, waarbij een aanzienlijke kans bestaat op verlies of onrechtmatige verwerking van *persoonsgegevens* die door AK+ wordt verwerkt, dan wel dat verlies of onrechtmatige verwerking zich voordoet, zal AK+ daarvan melding doen bij de gegevensverantwoordelijke. Betreft het een inbreuk op de beveiliging die betrekking heeft op gegevens waarvoor AK+ zelf gegevensverantwoordelijk is dan zal deze worden gemeld bij de Autoriteit Persoonsgegevens (AP). Tenzij kan worden aangetoond dat het onwaarschijnlijk is dat deze inbreuk risico’s voor de rechten en vrijheden van natuurlijke personen met zich brengt. Zie *bijlage 4 - Protocol beveiligingsincidenten en datalekken*voor een overzicht van de gehanteerde beoordelingscriteria.

AK+ zal iedere datalek waarbij persoonsgegevens verloren zijn gegaan of ongeoorloofd zijn gewijzigd, verstrekt of ingezien, ongeacht of het moet worden gemeld, documenteren *(bijlage 3 - Formulier registratie datalekken).* Het overzicht hoeft niet openbaar te worden gemaakt.

8.2 Vaststellen + werkwijze datalekken

Voor een specifieke toelichting en/of uitwerking om vast te stellen of er sprake is van een inbreuk op de beveiliging en/of een datalek, en of daarvan een melding moet worden gedaan bij de AP dan wel betrokkene(n), hanteert AK+ de beoordelingscriteria die zijn opgenomen in *bijlage 4 - Protocol beveiligingsincidenten en datalekken*.

Daarnaast heeft AK+ met de klant in een verwerkersovereenkomst afspraken gemaakt met betrekking tot de werkwijze bij een inbreuk in de beveiliging en/of een datalek.

Artikel 9 - Klachten

Indien betrokkene van mening is dat de AVG, overige wet- en regelgeving en de bepalingen in het privacyreglement niet worden nageleefd, dient zij zich te wenden tot de coördinator informatiebeveiliging.

Als de klacht voor betrokkene niet leidt tot een voor hem/haar acceptabel resultaat, kan hij/zij zich wenden tot de AP.

Artikel 10 – Inwerkingtreding en wijziging

Dit reglement treedt in werking in 01-05-2018 en is vastgesteld door AK+. Het privacyreglement zal indien gewenst of nodig worden geëvalueerd om de AVG correct na te leven.

Bijlage

Bijlage 1 - Privacyverklaring

Vanaf mei 2018 dienen alle organisaties te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). De belangrijkste uitgangspunten van de AVG zijn transparantie en verantwoording. Voor u als betrokkene moet het duidelijk zijn wat er met uw persoonsgegevens gebeurt. In een zo vroeg mogelijk stadium moet u hierover worden geïnformeerd. AK+ neemt privacy serieus. In deze verklaring leggen wij uit hoe wij omgaan met informatie (persoonsgegevens) van ons personeel.

### Privacyregels AK+

AK+ heeft privacyregels opgesteld. Deze regels zijn opgeschreven in een privacyreglement en voldoen aan nationale en internationale privacywetgeving. U kunt dit reglement vinden in de kast op kantoor. Hierin is vastgelegd welke gegevens we verzamelen, waarom we dit doen, wie toegang heeft tot de gegevens en hoe we deze informatie beschermen. Komt u in deze verklaring iets tegen waar u meer over wilt weten: raadpleeg dan eerst het privacyreglement.

Welke informatie verwerkt AK+?
AK+ heeft informatie over wie u bent (naam, geboortedatum- en plaats, geslacht, nationaliteit, kopie ID-bewijs) en uw bankrekening-, contact- en adresgegevens. Ook hebben wij gegevens die zien op de beoordeling van uw werkzaamheden en gegevens met het oog op uw arbeidsomstandigheden en veiligheid. Daarnaast verwerkt AK+ beeldmateriaal waar u mogelijk op te zien bent, zoals (pas)foto’s en videobeelden van de beveiligingscamera’s.

Verder maken wij als u bij AK+ komt werken een personeelsnummer en inloggegevens voor u aan, zodat u het netwerk van AK+ kunt gebruiken en eventueel toegang hebt tot het financiële- en/of salarisverwerkingssysteem. Deze informatie en ook gegevens over uw activiteiten binnen het netwerk van AK+ (salarisverwerkingssysteem, inloggegevens) slaan wij op. Ook verzamelt AK+ verschillende gegevens van haar medewerkers die nodig zijn om te kunnen voldoen aan verzoeken van opdrachtgevers.

### Waarom heeft AK+ deze informatie nodig?

AK+ gebruikt uw persoonsgegevens alleen met het oog op uw arbeidsovereenkomst en de uitvoering van uw werkzaamheden en/of het verwerken van uw salaris. Informatie over u wordt alleen gebruikt voor doelen die hiermee te maken hebben. Denk aan het aangaan en beëindigen van uw arbeidsovereenkomst, het vaststellen en uitvoeren van uw arbeidsvoorwaarden, het uitvoeren van re-integratieactiviteiten, het toepassing geven aan geldende wet- en regelgeving en andere voorkomende personeelszaken. Ook worden u persoonsgegevens gebruikt in het kader van toezicht en beveiliging.

AK+ gebruikt persoonsgegevens voor deze doelen alleen als dit volgt uit de arbeidsovereenkomst, de wet of andere wet- en regelgeving of specifieke eisen die binnen de branche worden gesteld of noodzakelijk zijn.

### Hoe komt AK+ aan de informatie?

In de meeste gevallen levert u zelf informatie aan wanneer u werkzaamheden gaat uitvoeren voor AK+. Ook houdt AK+ zelf informatie bij. Bijvoorbeeld over uw aanwezigheid en functioneren binnen AK+ en/of op de (werk)locaties/scholen, waarmee AK+ een dienstverleningsovereenkomst heeft gesloten. Daarnaast ontvangt AK+ gegevens van derden, bijvoorbeeld informatie van de arbodienst, de Arboarts of een ingeschakelde adviserende partij die noodzakelijk is met het oog op re-integratie of uw functie-uitoefening.

### Geeft AK+ mijn persoonsgegevens ook aan iemand anders?

Ja, maar slechts in beperkte gevallen. Wij zijn wettelijk verplicht sommige gegevens te delen met de overheid en wij geven gegevens over u aan de politie of zorgverleners als dit nodig is (bijvoorbeeld bij een ongeval). Als u in naam van AK+ werk verricht voor een derde partij (bijvoorbeeld een klant)  ontvangen ook zij de informatie die zij daarvoor nodig hebben. Met de schoolbesturen/samenwerkingsverband(en)/opdrachtgevers sluit AK+ een
verwerkersovereenkomst, zodat de persoonsgegevens van het personeel van beide partijen over en weer - en dus ook bij derde partijen - goed beschermd zijn.

### Hoelang worden mijn gegevens bewaard?

AK+ bewaart persoonsgegevens op servers en op papier niet langer dan nodig is. AK+ kijkt altijd eerst waarom de gegevens zijn verzameld en besluit dan hoe lang ze worden bewaard. De meeste informatie wordt (uiterlijk) 2 jaar na het einde van uw dienstverband verwijderd. Soms is het echter nodig om gegevens langer te bewaren, bijvoorbeeld omdat dit verplicht is op basis van een wet (denk bijvoorbeeld aan een deel van de loonadministratie op last van de Belastingdienst).

### Welke rechten heb ik?

U hebt het recht om periodiek, met redelijke tussenpozen, een verzoek tot inzage te doen in uw dossier. U ontvangt van ons een overzicht van de gegevens die wij van u hebben. Ook bent u gerechtigd AK+ te verzoeken om gegevens aan te passen als u van mening bent dat informatie niet klopt of onvolledig is. AK+ is verplicht om persoonsgegevens te wissen of niet meer te gebruiken als de gegevens niet meer nodig zijn of als u bezwaar maakt tegen het gebruik daarvan.

Daarnaast heeft u het recht om de gegevens die u zelf ooit aan AK+ heeft verstrekt, mee te nemen. AK+ zorgt ervoor dat deze gegevens op uw verzoek in een makkelijk mee te nemen vorm aan u worden afgegeven.

Bent u van mening dat AK+ niet zorgvuldig omgaat met uw persoonsgegevens? Neem dan eerst contact op met AK+ om uw zorgen te bespreken. Meer informatie over uw rechten kunt u in artikel 5 van het privacyreglement vinden.

### Vragen? Neem contact op met de coördinator informatiebeveiliging

Als u vragen heeft of meer wilt weten over privacy bij AK+ kunt u contact opnemen met de coördinator informatiebeveiliging. De coördinator informatiebeveiliging binnen de organisatie is Frank Verhallen en u kunt hem bereiken via frank@akplus.nl.

---------------------------------------------------------------------------------------------------

**Privacyverklaring**

In geen geval zal AK+ uw persoonlijke gegevens delen voor andere doeleinden dan in het privacyreglement is opgenomen.

Hierbij geef ik AK+ toestemming om mijn persoonsgegevens, voor de doelen/grondslagen opgenomen in het privacyreglement, te registreren.

**Naam:

Plaats:

Datum:

Handtekening:**

Bijlage 2 - Formulier melding datalekken

Dit formulier bevat een aantal onderdelen die moeten worden opgegeven als er een datalek is geweest en hiervan een melding wordt gemaakt aan Autoriteit Persoonsgegevens (AP) en/of klanten.

Gegevens over het datalek

1. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan?
2. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
Minimaal:
Maximaal:
3. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk?
4. Wanneer vond de inbreuk plaats en, indien van toepassing, hoelang heeft de inbreuk plaatsgevonden?
5. Wat is de aard van de inbreuk (meerdere mogelijkheden)?
- Lezen (vertrouwelijk)
- Kopiëren
- Veranderen (integriteit)
- Verwijderen of vernietigen (beschikbaarheid)
- Diefstal
- Vooralsnog onbekend
6. Om welk type persoonsgegevens gaat het (meerdere mogelijkheden)?
- Naam-, adres- en woonplaatsgegevens
- Telefoonnummers
- E-mailadressen of andere adressen voor elektronische communicatie
- Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
- Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
- Burgerservicenummer (BSN)
- Paspoortkopieën of kopieën van andere legitimatiebewijzen
- Geslacht, geboortedatum en/of leeftijd
- Bijzondere persoonsgegevens
- Eventueel overige gegevens.
7. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen (meerdere mogelijkheden)?
- Stigmatisering of uitsluiting
- Schade aan de gezondheid
- Blootstelling aan (identiteits)fraude
- Blootstelling aan spam of phishing
- Eventueel anders.

Vervolgacties

1. Welke technische en organisatorische maatregelen heeft AK+ getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Technische beschermingsmaatregelen

1. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
	1. Ja, want
	2. Nee, want
	3. Deels, namelijk:

Inlichten van de betrokkenen

1. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
	1. Ja, want
	2. Nee, want
	3. Onbekend
2. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen?
	1. Ik heb het datalek aan de betrokkenen gemeld op [DD-MM-JJJJ]
	2. Ik ga het datalek aan de betrokkenen melden op [DD-MM-JJJJ]
	3. Onbekend
3. Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen en welk communicatiemiddel(en) gebruikt u hiervoor of gaat u gebruiken?
4. Indien van toepassing, waarom ziet u af van het melden van het datalek aan de betrokkenen?
	1. De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten.
	2. Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want:
	3. Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk
	4. Anders, namelijk:

Internationale aspecten

1. Heeft de inbreuk betrekking op personen in andere EU-landen
	1. Ja
	2. Nee
	3. Onbekend
2. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
	1. Ja, namelijk:
	2. Nee

Slot

1. Is naar uw mening deze melding compleet?
	1. Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
	2. Nee, deze melding wordt later nog uitgebreid met aanvullende informatie over deze inbreuk.

Bijlage 3 - Formulier registratie datalekken

Dit formulier wordt *standaard* ingevuld bij elke datalek waarvan geen melding wordt gemaakt.

**1) Wanneer vond het lek plaats?**

**2) Wat is er met de gegevens gebeurd? (verloren gegaan / door een onbevoegde ingezien / gekopieerd / gewijzigd)**

**3) Van wie (welke groepen) zijn gegevens gelekt?**

**4) Om hoeveel personen gaat het?**

**5) Om welke persoonsgegevens gaat het?**

**6) Wat zijn de (mogelijke) gevolgen van de inbreuk? (bijvoorbeeld risico op identiteitsfraude of reputatieschade)**

**7) Welke maatregelen zijn genomen naar aanleiding van het lek? (schadebeperking)**

**8) Welke maatregelen zijn genomen om te zorgen dat het niet nog een keer kan gebeuren?**

Bijlage 4 - Protocol beveiligingsincidenten en datalekken

**Artikel 1 - Doel van dit protocol**

Het protocol is bedoeld om het personeel bewust te maken over het verschil tussen een inbreuk op de beveiliging en een datalek. Tegelijkertijd wordt in het protocol duidelijk gemaakt in welke gevallen en zo ja, op welke wijze aan wie of welke instantie een melding moet worden gemaakt.

**Artikel 2 - Begrippen**

*Beveiligingsincident:*is een inbreuk op de beveiliging die *mogelijk* leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens.

*Datalek:* is een inbreuk op de beveiliging die *wel* leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens.

**Artikel 3 - Persoonsgegevens**

Persoonsgegevens zijn direct identificerende gegevens (naam, adres, woonplaats of BSN-nummer). Indirect identificerende gegevens zijn gegevens die iets zeggen over een persoon, omdat zij gekoppeld kunnen worden aan een direct persoonsgegeven. Als er kan worden achterhaald om welke persoon het gaat, is er sprake van een persoonsgegeven.

*Voorbeelden: telefoonnummer, e-mailadres, salarisgegevens, gegevens met betrekking tot ziekte en gezondheid, functionerings- en beoordelingsgesprekken, betalingsachterstanden en gegevens over gezinssituatie etc.*

**Artikel 4 - Beveiligingsincidenten**

**4.1 Niet bewuste incidenten zonder opzet**

* Het laten liggen en/of verliezen van een laptop, tablet, mobiele telefoon, USB-stick of papieren dossier;
* Ruimtes en/of kasten binnen de organisatie met daarin fysieke dossiers die per ongeluk niet op slot hebben gezeten voor een bepaalde periode;
* Onbeheerd accounts open laten staan en/of laptop en/of computer achterlaten met daarop een memo-sticker met inlognaam en wachtwoord;
* Het verzenden van een e-mail met vertrouwelijke gegevens aan de verkeerde ontvanger;
* Het crashen van een harde schijf met daarop persoonsgegevens;
* Brand in een serverruimte, datacentrum of de opslagplaats (archief) van de organisatie;
* Als één van de hiervoor genoemde situaties zich voordoet bij een (sub)verwerker van AK+.

**4.2 Bewuste incidenten met opzet**

* Fysieke diefstal van een laptop, tablet, mobiele telefoon, USB-stick of (onderdelen van een) papieren dossier;
* Het kopiëren, meenemen of vernietigen van persoonsgegevens door personeel bijvoorbeeld uit onvrede over ontslag, functionerings- en/of beoordelingsgesprek, als vriendendienst of als gevolg van chantage;
* Phishing: het uitbuiten van menselijke kwetsbaarheden door hen onder valse voorwendselen persoonsgegevens te ontfutselen via mail of internet;
* Hack: het uitbuiten van kwetsbaarheden in informatiesystemen en webservers;
* Als één van de hiervoor genoemde situaties zich voordoet bij een (sub)verwerker van AK+.

**4.3**

Indien zich een dergelijk of soortgelijk onbewust of bewust incident voordoet, is er sprake van een beveiligingsincident en dient het personeel dit te melden aan de coördinator informatiebeveiliging. Indien het om (persoons)gegevens gaat waar AK+ de (sub)verwerker van is, dient er ook een melding te worden gemaakt aan de Functionaris Gegevensbescherming van de verwerkingsverantwoordelijke.

**4.4**

Heeft het beveiligingsincident geen betrekking op de verwerking van persoonsgegeven(s), dan is de AVG en daarmee de meldplicht niet van toepassing.

**Artikel 5 - Vernietigd en verloren**

**5.1**

Persoonsgegevens zijn weg en niet meer reproduceerbaar. De organisatie beschikt (ook) niet meer over een complete en actuele reservekopie van de persoonsgegevens en daarom is er sprake van een datalek.

**5.2**

Er is niet direct sprake van een datalek als er van de verloren en/of vernietigende persoonsgegeven(s) nog een actuele reservekopie beschikbaar is.

**Artikel 6 - Onrechtmatig**

**6.1**

In meerdere situaties kan sprake zijn van onrechtmatige verwerking. Het kan gaan om onbevoegde (1) aantasting, (2) wijziging, (3) kennisneming en (4) doorzending/ verstrekking van persoonsgegevens.

**6.2**

Als niet kan worden uitgesloten dat de inbreuk op de beveiliging heeft geleid tot een onrechtmatige verwerking, dan moet het worden beschouwd als een datalek. Is er sprake van een software-besmetting op het systeem dan moet er in ieder geval van een datalek worden uitgegaan.

**Artikel 7 - Datalekken**

**7.1**

Als het om een datalek van persoonsgegevens gaat, waar AK+ als (sub)verwerker bij betrokken is, hoeft zij in beginsel geen melding te maken aan de AP en/of betrokkene(n). Het is echter wel van belang dat AK+, de Functionaris Gegevensbescherming van de verwerkingsverantwoordelijke inlicht, in die gevallen waarin AK+ zou handelen *alsof zij* de verwerkingsverantwoordelijke is. Zie *artikel 7* van de verwerkersovereenkomst voor de specifiek gemaakte afspraken tussen de verwerkingsverantwoordelijke en AK+.

**7.2**

Indien het gaat om een datalek met persoonsgegevens van het personeel van AK+, waarvan AK+ in die hoedanigheid de verwerkingsverantwoordelijke is, geldt het voorgaande niet en zal namens AK+, na overleg met haar directeur en de coördinator informatiebeveiliging, onverwijld een melding moeten worden gemaakt aan de AP en mogelijk ook aan de betrokkene(n), indien:

**“De datalek leidt tot (een aanzienlijke kans op) ernstige nadelige**
**gevolgen voor de bescherming van de persoonsgegevens”.**

Van het voorgaande is in elk geval sprake als het persoonsgegevens van *gevoelige aard* betreffen.

Persoonsgegevens van *gevoelige aard* zijn onder andere:

* Gegevens over de financiële of economische situatie van betrokkene, zoals (problematische) schulden, salaris- en betalingsgegevens;
* Gegevens die kunnen leiden tot stigmatisering of uitsluiting, zoals privé- of werk- problemen, verslagen functionerings- en beoordelingsgesprekken;
* Gebruikersnamen, wachtwoorden en andere inloggegevens, waarbij het van belang is tot welke persoonsgegevens of de verwerking ervan, de inloggegevens toegang geven;
* Gegevens die kunnen worden misbruikt voor (identiteits)fraude, zoals kopieën van identiteitsbewijzen en het Burgerservicenummer (BSN).

**“Een inbreuk risico’s voor de rechten en vrijheden van betrokkene(n) met zich mee brengt”.**

Bij het voorgaande dient de aard en de omvang van het datalek in ogenschouw te worden genomen.
*Voorbeelden: een datalek bij grote instellingen zoals de Belastingdienst dat kan leiden tot financieel nadeel of tot compromittering (in gevaar brengen) van persoonsgegevens die worden beschermd door een geheimhoudingsplicht en een datalek in omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt.*

Daarnaast is relevant:

* Of er sprake is van veel persoonsgegevens per persoon en/of persoonsgegevens van grote groepen betrokkenen, omdat deze aantrekkelijk voor misbruik in het criminele circuit zijn;
* De mate van ingrijpen van de beslissing(en) die op basis van de verwerkte persoonsgegevens wordt genomen. Hoe ingrijpender, hoe groter de impact;
* Of er omvangrijke verwerkingen zijn die binnen ketens worden gedeeld. De gevolgen van verlies of onbevoegde wijziging kunnen door de hele keten optreden, waardoor het moeilijker is om de situatie te overzien.

**7.3**

Het *‘onverwijld melden’* aan AP dan wel aan de verwerkingsverantwoordelijke, houdt in dat AK+ enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. Wat als ‘onverwijld’ moet worden aangemerkt hangt verder af van de omstandigheden van het geval. Is er sprake van een klein en overzichtelijk datalek, dan mag worden verwacht dat sneller na de ontdekking wordt gemeld, dan in geval van een omvangrijke datalek waarbij langdurig grote hoeveelheden data vanuit verschillende bestanden en servers is gekopieerd. Het AP hanteert een uiterlijke meldplicht van 72 uur. *Let op:* in de verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en AK+ als (sub)verwerker is een uiterlijke meldplichtduur van 36 uur opgenomen.

**Artikel 8 - Melden aan betrokkene(n)**

**8.1**

Een melding aan betrokkene(n) kan achterwege blijven als de toegepaste cryptografie (versleuteling) en/of andere adequate technische beschermingsmaatregelen (remote wipe, pseudonimisering) voldoende bescherming biedt om uit te kunnen sluiten dat het datalek een hoog risico inhoudt. Dat wil zeggen dat het om persoonsgegevens moet gaan, die onbegrijpelijk of ontoegankelijk zijn gemaakt voor eenieder die geen recht op kennisname heeft.
*Let op:* tegen persoonsgegevens die zijn blootgesteld aan vernietiging of aantasting, biedt versleuteling niet voldoende bescherming om een melding aan betrokkene achterwege te laten.

**8.2**

Het is aan de AK+ om te beoordelen of de versleuteling sterk genoeg is en op de juiste wordt uitgevoerd.

**8.3**

Als het datalek waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkene inhouden én de mededeling geen onevenredige inspanningen vergen en/of de melding een onderzoek naar de omstandigheden van een datalek niet nodeloos hinderen, dan moet het datalek aan betrokkene *altijd schriftelijk* worden gemeld. Mocht er wel sprake zijn van nodeloos hinderen, dan dient zodra dat is opgeheven alsnog een melding aan betrokkene gedaan te worden.

**8.4**

Met een datalek kunnen de belangen van betrokkene zowel materieel als immaterieel worden geschaad. Denk aan:

* Schending van de vertrouwelijkheid (financiële of fysieke schade, reputatie- of identiteitsschade, chantage of misbruik van inloggegevens);
* Beschikbaarheid (bepaalde diensten of activiteiten kunnen niet meer worden verleend of uitgevoerd en rechten - verwijdering of rectificatie - kunnen ook niet meer worden uitgeoefend);
* Integriteit (niet in overeenstemming met de werkelijkheid: onterechte beslissingen).

**8.5**

Het is aan de directeur en de coördinator informatiebeveiliging van AK+ om te beoordelen of een datalek aan betrokkene wordt gemeld. Indien het gaat om een datalek van persoonsgegevens van gevoelige aard (artikel 7), dan moeten zij ervan uitgaan dat het datalek - niet alleen aan AP - maar ook aan de betrokkene moet worden gemeld. In de overige gevallen zullen de directeur en de coördinator informatiebeveiliging een afweging moeten maken op basis van de omstandigheden van het geval. Ook vragen zij zich af hoe groot het risico is dat de mogelijke nadelige gevolgen daadwerkelijk optreden. Zijn er voor betrokkene daadwerkelijk ongunstige gevolgen voor de persoonlijke levenssfeer, dan is het informeren van betrokkene noodzakelijk. Tot slot kan ook AP van AK+ verlangen dat alsnog een kennisgeving wordt gedaan. Tegen dit besluit staat bezwaar en beroep open.

**8.6** Het *‘onverwijld melden’* aan betrokkene betekent zonder onredelijke vertraging. De termijn is afhankelijk van de aard van het risico. Hoe acuter, hoe sneller de mededeling moet worden gedaan. Daarnaast geldt ook hetgeen hierover in **7.3**is opgenomen.