



Reglement gebruiksregels ICT-faciliteiten

(Acceptable Use Policy)

Amsterdam,
december 2013

Ferry J. de Jong
Hoofd ICT



Inhoudsopgave

Reglement gebruiksregels ICT-faciliteiten (Acceptable Use Policy)	3
Begripsbepalingen.....	3
Artikel 1. Toepasbaarheid.....	3
Artikel 2. Algemene bepalingen.....	4
Artikel 3. Gebruik ICT-faciliteiten	4
3.1 Algemeen	4
3.2 ICT ruimten	4
3.3 Gebruik apparatuur in AHK ruimten.....	4
3.4 Gebruik AHK netwerk, wireless	5
3.5 Gebruik AHK netwerk, bedraad	5
3.6 Gebruik computerlokalen en studielandschappen.....	5
Artikel 4. Gebruik gebruikersnaam/wachtwoord	5
Artikel 5. Gebruik e-mail	5
Artikel 6. Gebruik internet	6
Artikel 7. Opslag van informatie.....	6
Artikel 8. Auteursrecht	6
Artikel 9. Commercieel gebruik.....	7
Artikel 10. Privé gebruik.....	7
Artikel 11. Controle op naleving gebruiksregels	7
Artikel 12. Rapportage	7
Artikel 13. Bewaren van persoonsgegevens, inzage en klachten	8
Artikel 14. Controle	8
Artikel 15. Sanctiebepalingen	9
Artikel 16. Registratie van gegevens ten behoeve van evaluatie.....	9
Artikel 17. Slotbepalingen	9
Artikel 18. Accordering.....	9



Reglement gebruiksregels ICT-faciliteiten (Acceptable Use Policy)

Dit reglement "Reglement gebruiksregels ICT-faciliteiten (Acceptable Use Policy)", verder genoemd reglement beperkt zich tot ICT-faciliteiten. Regels voor het gebruik van RSI preventie en dergelijke worden buiten beschouwing gelaten.

Dit document is opvolgend aan en vervangt het document "Reglement gebruiksregels ICT" met een ingangsdatum van 1 maart 2006.

Begripsbepalingen

In dit reglement wordt verstaan onder:

Werknemer	eenieder die en arbeidsovereenkomst heeft met AHK
Student	eenieder die als student staat ingeschreven bij AHK
Cursist	eenieder die als cursist staat ingeschreven bij AHK
Bezoeker	eenieder die rechtmatig gebruik maakt van de gastvrijheid van AHK
Gebruiker	de werknemer, student/cursist of bezoeker die rechtmatig toegang heeft verkregen tot of rechtmatig gebruik maakt van de ICT-faciliteiten van AHK
Toezichthouder	de verantwoordelijke functionaris in de functie van Hoofd ICT die namens het College van Bestuur de gemandateerde taak heeft toezicht te houden op het gebruik van faciliteiten en in het kader daarvan gerechtigd is regels op te stellen en instructies en aanwijzingen te geven
Beheerder	de verantwoordelijke functionaris die namens de toezichthouder belast is met het verzorgen van de toegankelijkheid, configuratie, continuïteit en beveiliging van een ICT-faciliteit
ICT-faciliteiten	de door of namens AHK ter beschikking gestelde faciliteiten voor elektronische informatie uitwisseling, waaronder Intranet, Internet, World Wide Web, elektronische leeromgeving, e-mail, e-mailadres, en alle faciliteiten al dan niet met een gebruikersnaam/wachtwoord beschikbaar, evenals (draadloze) aansluitfaciliteiten ten behoeve van notebooks. Het betreft hier dus zowel apparatuur als programmatuur als verbindingen. De omschrijving van ICT-faciliteiten is niet limitatief en kan worden aangevuld met faciliteiten zoals in de toekomst door AHK ter beschikking worden gesteld
Toegangscade	het samenstel van een gebruikers- of login naam en bijbehorend wachtwoord
E-mailadres	de door AHK aan gebruiker toegekende unieke code ter aanduiding van zijn "elektronisch" postvak Mailbox: ruimte, ingericht op een opslagmedium van een computer die exclusief ter beschikking staat van de gebruiker voor ontvangst, opslag en verzending van elektronische post
WBP	Wet Bescherming Persoonsgegevens
WHW	Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

Artikel 1. Toepasbaarheid

1. Dit reglement is van toepassing op alle medewerkers, studenten en bezoekers van AHK die gebruik maken van de ICT-faciliteiten van AHK.



Artikel 2. Algemene bepalingen

1. Gebruik van de ICT-faciliteiten dient binnen de grenzen van de wet plaats te vinden (in het bijzonder zijn diefstal, fraude, ongeautoriseerd binnendringen in computersystemen van derden, schending van auteursrechten en valsheid in geschrifte verboden).
2. De continuïteit van het primaire proces en/of de bedrijfsvoering van AHK mag nimmer in gevaar komen.
3. Het ophalen en/of verspreiden van discriminerende uitingen is niet toegestaan.
4. Gebruik van de faciliteiten moet in lijn zijn met de primaire doelstellingen of de bedrijfsvoering van AHK.
5. Het ontplooiën van activiteiten die de goede naam van AHK kunnen schaden zijn niet toegestaan.

Artikel 3. Gebruik ICT-faciliteiten

3.1 Algemeen

1. De toegang tot of het gebruik van deze faciliteiten kan worden beperkt door het management.
2. Bij het gebruik van computers en netwerkfaciliteiten wordt de zorgvuldigheid in acht genomen. Gebruikers hebben hierin hun eigen verantwoordelijkheid.
3. Gebruik van de faciliteiten is primair bedoeld voor studie en arbeid. Binnen redelijke grenzen is privégebruik toegestaan, een en ander voor zover de goede voortgang van de dagelijkse activiteiten aan de AHK en het netwerk en het netwerkverkeer daardoor niet worden gehinderd.
4. De toegang tot of het gebruik van de ter beschikking gestelde faciliteiten kan worden beperkt door het management.
5. Gebruiker dient licentiebepalingen van de door AHK ter beschikking gestelde faciliteiten na te leven en te respecteren.
6. Gebruiker is verplicht om aanwijzingen van de ICT beheerder voor het gebruik van deze faciliteiten op te volgen.
7. Gebruiker verplicht zich te onthouden van activiteiten die het belang van AHK, andere gebruikers of een goede werking van de faciliteiten zelf kunnen schaden.

3.2 ICT ruimten

ICT ruimten zijn ruimtes waar ICT apparatuur geïnstalleerd staat of waar ICT medewerkers werken voor het directe beheer van het netwerk. Dit zijn de specifieke ICT kantoorruimtes en de Slave Equipment Room (SER) en Master Equipment Room (MER). Een SER en MER zijn ICT ruimtes waar ICT apparatuur is opgesteld.

1. Niemand zal ICT ruimten betreden zonder goedkeuring van de ICT medewerkers behoudens personen die om AHK beheerredenen in de ruimtes moeten zijn.
2. Personen die om AHK beheerredenen wel in de ruimte aanwezig moeten zijn voor bijvoorbeeld onderhoud aan de ruimte zullen de ICT apparatuur niet aanraken of beroeren. Voor het betreden van de ICT ruimte maken zij een afspraak met de afdeling ICT.
3. Zelfs als daar wel de gelegenheid toe is, zal de gebruiker deze ruimte niet betreden

3.3 Gebruik apparatuur in AHK ruimten

1. Het is de gebruiker niet toegestaan apparatuur los te koppelen of te verplaatsen.
2. Het is de gebruiker niet toegestaan apparatuur te wijzigen. Indien apparatuur door gebruikers mag worden gewijzigd staat dat beschreven in het ICT gedeelte op de AHK website (www.ahk.nl).
3. Het is gebruiker niet toegestaan om zonder toestemming van de ICT beheerder de instellingen van de apparatuur te wijzigen.
4. Het is gebruiker niet toegestaan om zonder toestemming van de ICT beheerder systeem software of applicaties toe te voegen of te wijzigen.



5. Het is niet toegestaan de beschikbaar gestelde ICT apparatuur zodanig te gebruiken, te verlaten of achter te laten dat anderen in de gelegenheid worden gesteld om hier misbruik van te maken.
6. Apparatuur wordt als het niet gebruikt wordt uitgeschakeld door de gebruiker (Green ICT).

3.4 Gebruik AHK netwerk, wireless

1. Het gebruik op het netwerk van (eigen meegebrachte) "notebooks", tablets, smartphones en dergelijke is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen.
2. Het is niet toegestaan het (wireless) netwerk onnodig te belasten.

3.5 Gebruik AHK netwerk, bedraad

1. Het aansluiten van apparatuur op het AHK netwerk is een verantwoordelijkheid van de ICT afdeling.
2. De afdeling ICT stelt de outlet (netwerkaansluitpunt) beschikbaar.
3. De afdeling ICT sluit apparatuur aan en verwijderd de aansluiting met het netwerk.
4. Het aanwezig zijn van een outlet geeft de gebruiker niet het recht zelf apparatuur aan te sluiten.
5. Het is niet toegestaan het netwerk onnodig te belasten.

3.6 Gebruik computerlokalen en studielandschappen

1. Het gebruik van computerlokalen en studielandschappen is een verantwoordelijkheid van de faculteit. De gebruiker dient de regels die gesteld zijn door de faculteit te volgen.

Artikel 4. Gebruik gebruikersnaam/wachtwoord

1. De door AHK verstrekte gebruikersnamen en wachtwoorden zijn persoonlijk.
2. Eventuele afzonderlijke fysieke items ten behoeve van zware authenticatie (tokens, smart cards, e.d.) blijven eigendom van AHK en mogen alleen gebruikt worden voor het verkrijgen van toegang tot voorzieningen waar ze voor uitgegeven zijn.
3. Het is niet toegestaan een persoonlijk wachtwoord aan derden bekend te maken in welke vorm dan ook.
4. Het is niet toegestaan om zich met andere dan de persoonlijk toegekende gebruikersnamen en wachtwoorden toegang te verschaffen of pogingen te ondernemen andere gebruikersnamen en wachtwoorden te verkrijgen.
5. Gebruiker is verantwoordelijk voor alle acties die met het gebruik van zijn gebruikersnaam/wachtwoord zijn uitgevoerd, tenzij wordt aangetoond dat gebruikersnaam/wachtwoordcombinatie onrechtmatig door een ander verkregen is.
6. Gebruiker is verplicht de combinatie van de aan hem toegekende gebruikersnaam en persoonlijk wachtwoord zorgvuldig te beheren
7. Gebruiker dient regelmatig het persoonlijke wachtwoord te wijzigen en daarbij niet eenvoudig te raden wachtwoorden te kiezen.
8. Indien gebruiker het vermoeden heeft dat een persoonlijke gebruikersnaam/wachtwoordcombinatie in handen van anderen is gevallen, dient hij hiervan onmiddellijk de beheerder in kennis te stellen en relevante maatregelen te treffen die onbevoegd gebruik verder voorkomen.

Artikel 5. Gebruik e-mail

1. Het door AHK aan gebruiker ter beschikking gestelde e-mailadres is persoonlijk en niet overdraagbaar.
2. Het is gebruiker niet toegestaan om een niet voor hem geldend e-mailadres te gebruiken.
3. Het is verboden om zonder toestemming voor andere gebruiker bestemde e-mailberichten te lezen, te kopiëren, te wijzigen of te wissen.
4. Het is verboden zich toegang te verschaffen tot e-mailberichten van andere gebruikers



5. Het is niet toegestaan om e-mailberichten te ondertekenen met gebruikmaking van een andere naam.
6. Het is niet toegestaan om via de e-mailfaciliteiten van AHK berichten te versturen met een onzedelijke discriminerende, commerciële of bedreigende inhoud.
7. Commercieel gebruik van e-mail en het gebruik van e-mail voor, in welke vorm of voor welk doel dan ook, is niet toegestaan.
8. Het is zonder uitdrukkelijke toestemming van het bevoegde management niet toegestaan e-mail berichten te versturen aan meer dan 50 adressen tegelijkertijd.
9. Voor het tegengaan van virussen en andere schadelijke programma's, wordt het e-mailverkeer in het kader van systeem- en netwerkbeveiliging op geautomatiseerde wijze gecontroleerd.

Bij het in gebruikte systeem (VMware, Zimbra) wordt op de volgende geautomatiseerde wijze gecontroleerd op virussen en spam (status 16 augustus 2011).

Viruschecking:

1. Voor het checken op virus wordt binnen Zimbra gebruik gemaakt van ClamAV. ClamAV is een open source (GPL) antivirus engine ontworpen voor het vinden van Trojans, virussen, malware en andere kwaadwillige bedreigingen. Mail met virussen worden verwijderd.

Spam controle:

1. Er wordt gebruik gemaakt van gray-listing om te voorkomen dat spam de mailboxen van de AHK bereikt. Mail op deze manier gedetecteerd komt niet aan in Zimbra.
2. Binnen Zimbra wordt gebruik gemaakt van spam filtering met de open source oplossingen Spam Assassin en DSPAM. Spam ontdekt door beide oplossingen wordt doorgestuurd naar de Junk folder.

Artikel 6. Gebruik internet

1. Het is niet toegestaan om via de ICT-faciliteiten van AHK sites te bezoeken die pornografisch, seksueel getint, racistisch, discriminerend, beledigend, opruiend of ander aanstootgevend materiaal tonen noch hiervan te downloaden.
2. Zich zonder toestemming toegang te verschaffen tot niet openbare bronnen.
3. Informatie zonder toestemming van de rechthebbende te wijzigen of te vernietigen.

Artikel 7. Opslag van informatie

1. Gebruiker dient zich te vergewissen van de rechtmatigheid van de door hem opgeslagen informatie.
2. Niet alle opgeslagen informatie wordt per definitie door de beheerder gekopieerd voor back-up doeleinden. Gebruiker dient zich te vergewissen dat van zijn opgeslagen data een back-up wordt gemaakt en is, indien dit niet het geval is, hier zelf verantwoordelijk voor.
3. Gebruiker dient geen data op te slaan op de lokale harde schijf van de apparatuur van AHK. Zo dit toch gebeurt, dient hij/zij er zich van bewust te zijn dat deze voor iedere volgende gebruiker toegankelijk is en gewist mag worden.

Artikel 8. Auteursrecht

1. Gebruik van de ICT-faciliteiten waardoor schending van auteursrecht en of ander intellectueel eigendom plaatsvindt, bijvoorbeeld door het plaatsen van software, muziek, beeldmateriaal of boeken op servers, is niet toegestaan.
2. Gebruiker maakt geen kopieën van software en/of documentatie bij software waarvan AHK licentiehouders of licentieverstrekker is, zonder voorafgaande schriftelijke toestemming van AHK.



3. Gebruiker vrijwaart AHK van alle aansprakelijkheid voor schade die derden mochten ondervinden als gevolg van schending van het gestelde in dit artikel.

Artikel 9. Commercieel gebruik

1. Het is niet toegestaan om de ICT-faciliteiten van AHK te gebruiken voor privédoeleinden met een commercieel oogmerk. De vanwege AHK ter beschikking gestelde e-mail adressen mogen niet worden gebruikt voor commerciële verspreiding.
2. Het is niet toegestaan de ICT-faciliteiten van AHK te gebruiken voor commerciële doeleinden zonder uitdrukkelijke toestemming van de toezichthouder.

Artikel 10. Privé gebruik

1. De door AHK beschikbaar gestelde ICT-faciliteiten dienen te worden gebruikt ten behoeve van de functie-uitoefening of studie. Het is in beperkte mate toegestaan de ICT-faciliteiten van AHK voor privédoeleinden te gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden van gebruiker of van anderen, dit niet strijdig is met de overige bepalingen in dit reglement en dit de ICT-faciliteiten van AHK niet hindert.

Artikel 11. Controle op naleving gebruiksregels

1. De AHK kan ten behoeve van de handhaving van de hier gestelde gebruiksregels het gebruik van ICT-faciliteiten controleren en registreren.
2. Controle vindt plaats op grond van navolgende doelen:
 - a) het tegengaan van niet toegestaan gebruik
 - b) het begrenzen van gebruik anders dan voor studie en arbeid
 - c) het goed functioneren van computers en de daarop geïnstalleerde software en het netwerk alsmede het voorkomen van overbelasting van of storingen aan het netwerk
 - d) het beschermen van computers, netwerk en netwerkverkeer voor aanvallen van buiten af (systeem- en netwerkbeveiliging)
 - e) kosten- en capaciteitsbeheersing
 - f) het beschermen van de privacy van studenten en medewerkers
 - g) het voorkomen van negatieve publiciteit voor de AHK en haar belangen
 - h) het inperken van risico's in de sfeer van aansprakelijkheidsstellingen en vorderingen tot schadevergoeding
 - i) het voorkomen van schade aan derden
 - j) bewijs en archief
3. De AHK kan bepaalde soorten inkomend en uitgaand e-mailverkeer, met inbegrip van de bijlagen, blokkeren, in quarantaine plaatsen en waar nodig geacht van het netwerk of computers verwijderen. Materiaal dat is geplaatst op computers, homepage of opslagruimte dat moet worden beschouwd als niet toegestaan gebruik als bedoeld in artikel 3.5, kan worden verwijderd.
4. Uitgaande e-mailberichten kunnen desgewenst worden voorzien van een door de AHK vastgestelde disclaimer.
5. De AHK bepaalt de omvang van de aan studenten en medewerkers in gebruik gegeven e-mailbox en homepage faciliteiten. Bij overschrijding van de maximale omvang kunnen berichten van de server worden verwijderd.
6. Gebruik dat het netwerkverkeer belemmert of verstoort dan wel anderszins niet in overeenstemming is met de doelen waarvoor de faciliteiten zijn verleend, kan worden geblokkeerd.

Artikel 12. Rapportage

1. Over het gebruik van ICT-faciliteiten wordt periodiek gerapporteerd aan het College van Bestuur. Daarbij kan sprake zijn van het vastleggen en beoordelen van gegevens omtrent e-mailverkeer, bezochte internetsites en de daarmee samenhangende tijdsbesteding. Deze gegevens zijn niet herleidbaar tot individuele personen.



2. Steekproefsgewijs kan controle plaatsvinden van gebruik van ICT-faciliteiten op individueel niveau. Bij deze controle wordt gebruik gemaakt van controlemiddelen die het minst inbreuk maken op de privacy van de desbetreffende gebruiker, zoals het volume van e-mailverkeer en de aard van de bijbehorende bijlagen.
3. Indien op grond van de aldus verkregen informatie het vermoeden gewettigd is dat gebruik in strijd is met de in dit reglement geformuleerde gebruiksregels, bezien in samenhang met de controledoelstellingen als bedoeld in artikel 11.2, kan het College van Bestuur opdracht geven een nader onderzoek te starten naar het gebruik op individueel niveau. Het is aan het College van Bestuur om de directeur van de betreffende faculteit over het onderzoek te informeren. Ook signalen of klachten uit de organisatie dan wel afkomstig van derden kunnen aanleiding geven tot nader onderzoek.
4. De opdracht tot nader onderzoek op individueel niveau wordt gegeven aan daartoe geautoriseerde medewerkers die terzake van het onderzoek slechts bevoegd zijn tot hetgeen in de daartoe strekkende opdracht staat vermeld; zij rapporteren aan het College van Bestuur.
5. De gebruiker die het aangaat wordt over het nader onderzoek geïnformeerd zodra de omstandigheden dat naar het oordeel van het College van Bestuur toelaten.
6. Het nader onderzoek op individueel niveau kan inhouden controle en analyse van gegevens betreffende de inhoud van de opdrachtregels, elektronische correspondentie, het taalgebruik en de verdere inhoud, zoals fotomateriaal of andere afbeeldingen, evenals controle en analyse van de gegevens die de gebruiker op computer of anderszins heeft opgeslagen.
7. Verdere controle blijft achterwege indien de uit het nader onderzoek blijkende feiten het vermoeden als bedoeld in artikel 12.3 niet verder ondersteunen.
8. In beginsel kan geen onderzoek worden ingesteld naar e-mailverkeer van, aan en tussen medewerkers met een vertrouwensfunctie, leden van de medezeggenschapsraden en leden van het College van beroep voor de examens. Hetzelfde geldt ter zake van e-mailverkeer van en aan de arbodienst. Indien de omstandigheden daartoe evenwel dringend nopen kan het College van Bestuur anders beslissen.
9. De uitzondering als bedoeld in het voorgaande lid geldt niet voor de controle op de veiligheid van het berichtenverkeer.

Artikel 13. Bewaren van persoonsgegevens, inzage en klachten

1. Gegevens over e-mailverkeer en internetgebruik die herleidbaar zijn tot een individuele gebruiker kennen een bewaartermijn van ten hoogste zes maanden.
2. Op het recht op inzage in of verzoeken tot aanvulling, wijziging of verwijdering van de opgeslagen persoonsgegevens is artikel 9 van de Interne regeling persoonsgevoelige informatie AHK¹ als laatstelijk vastgesteld (1 september 2003) van overeenkomstige toepassing.
3. Klachten terzake van niet-naleving van dit reglement worden in behandeling gegeven van het College van Bestuur, met medeweten van de desbetreffende directeur.

Artikel 14. Controle

Misbruik en incidenten melden

1. Met inachtneming van de WBP worden ter voorkoming van beheer- en capaciteitsproblemen evenals ter voorkoming van misbruik door de beheerder de ICT-faciliteiten via geautomatiseerde processen gecontroleerd en wordt het netwerkverkeer gevolgd; hierbij zijn de gegevens niet tot personen te herleiden.
2. Met inachtneming van de WBP worden door de beheerder, via geautomatiseerde processen, gegevens over het gebruik van ICT-faciliteiten verzameld en verwerkt ten behoeve van trendanalyses over het gebruik; hierbij zijn de gegevens niet tot personen te herleiden.
3. Bij een vermeende overtreding van de regels kan, in opdracht van toezichthouder, (gedurende een korte periode en na consultatie van het College van Bestuur) een gerichte controle plaatsvinden; bij een geconstateerde overtreding wordt de betrokken

Reglement gebruiksregels ICT faciliteiten (AUP). Vastgesteld door het College van Bestuur op 11 december 2013 na positief advies van de Hogeschoolraad (d.d. 03 december 2013)



gebruiker hier zo spoedig mogelijk door het College van Bestuur/Directeur op aangesproken. Afhankelijk van de geconstateerde overtreding zullen er sancties worden opgelegd. Indien nodig of noodzakelijk zullen de bevoegde instanties worden ingelicht.

4. Medische gegevens en gegevens van personen met een vertrouwensfunctie zijn in beginsel uitgesloten van inhoudelijke controle.

Artikel 15. Sanctiebepalingen

1. Handelen in strijd met de gebruiksregels als in dit reglement bedoeld kan leiden tot het treffen van (disciplinaire) maatregelen.
2. Tegen studenten kunnen de navolgende maatregelen worden genomen: schorsing, ontzegging van de toegang tot gebouwen en terreinen van de AHK voor ten hoogste een jaar. Aan studenten op wie de regels van de WHW niet van toepassing zijn, kunnen ook andere maatregelen worden opgelegd.
3. Tegen medewerkers kunnen de navolgende maatregelen worden genomen: schorsing en disciplinaire maatregelen als bedoeld in de CAO-HBO. Aan medewerkers op wie de CAO-HBO niet van toepassing is, kunnen ook andere maatregelen worden opgelegd.
4. Behalve de maatregelen als genoemd in de voorafgaande leden kan uitsluiting van gebruik van ICT-faciliteiten worden opgelegd voor een dan te bepalen periode.
5. Het opleggen van sancties geschiedt door het College van Bestuur. Daartoe strekkende besluiten kunnen worden ondertekend door de faculteitsdirecteur respectievelijk de directeur Servicebureau.

Artikel 16. Registratie van gegevens ten behoeve van evaluatie

1. Het College van Bestuur draagt zorg voor een geanonimiseerde registratie van het ingestelde nader onderzoeken als bedoeld in artikel 12, het aantal en de aard van de in verband daarmee opgelegde sancties evenals het aantal klachten naar aanleiding van het niet naleven van dit reglement.

Artikel 17. Slotbepalingen

1. Dit reglement is tweejaarlijks onderwerp van evaluatie van het College van Bestuur en de Centrale Medezeggenschapsraad. De gegevens als bedoeld in artikel 16 worden bij die evaluatie betrokken.
2. Dit reglement kan worden aangehaald als "Reglement gebruiksregels ICT faciliteiten (Acceptabel Use Policy)".
3. Dit reglement treedt in werking na vaststelling door College van Bestuur.

Artikel 18. Accordering

Vastgesteld door het College van Bestuur op 11 december 2013 na positief advies van de Hogeschoolraad (d.d. 03 december 2013).

ⁱ Het desbetreffende artikel in de Interne regeling persoonsgevoelige informatie AHK luidt als volgt:

Artikel 9. Rechten van betrokkenen; inzagerecht

1. Elke betrokkene heeft het recht:
 - a. te vragen of over hem/haar persoonsgegevens in het bestand zijn opgenomen
 - b. te vragen om een overzicht daarvan, zo mogelijk met inlichtingen over de herkomst, aan hem/haar te verstrekken dan wel die te mogen inzien
 - c. te vragen of hem/haar betreffende gegevens in het jaar voorafgaande aan het verzoek uit het systeem aan derden zijn verstrekt
 - d. te vragen om een verklaring met bepaalde persoonsgegevens uit het bestand, waarvan de betrokkene aantoont deze nodig te hebben om aan derden te kunnen overleggen
 - e. te verzoeken de gegevens uit het overzicht te verbeteren, aan te vullen of te verwijderen, indien de gegevens naar het oordeel van betrokkene feitelijk onjuist, voor het doel van de



registratie onvoldoende of niet ter zake dienend zijn dan wel in strijd met een wettelijk voorschrift

2. Een verzoek wordt schriftelijk aan de beheerder gedaan. De beheerder voldoet binnen zes weken na ontvangst schriftelijk aan het verzoek als bedoeld in lid 1 onder a tot en met d. De beheerder bericht binnen drie maanden na ontvangst of en zo ja in hoeverre aan het verzoek als bedoeld in lid 1 onder e zal worden voldaan.
3. Indien de beheerder twijfelt aan de identiteit van de verzoeker, dan vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of, ingeval het een verzoek als bedoeld in lid 1 onder b of d betreft, of hij het overzicht in persoon kan afhalen onder overlegging van een geldig identiteitsbewijs.