

REGLEMENT BESCHERMING PERSOONSgegevens INZAKE MONITORING ELECTRONISCH DATAVERKEER

Artikel 1 – Begripsbepalingen

Voor de begripsbepalingen wordt verwezen naar de, door het College van Bestuur van de Regionale Opleidingen Centrum Amsterdam, 't-Sticht, Amersfoort op 26 augustus 2001 vastgestelde, Gedragscode Bescherming Persoonsgegevens.

Artikel 2a – Aard en doel van de verwerking

Het doel van de monitoring van het elektronisch dataverkeer is het verwerken van persoonsgegevens ten behoeve van:

- De beveiliging en bescherming van de aanwezige informatietechnologie en informatie-infrastructuur;
- De preventie en sanctionering van ongewenst gebruik (volgens de uitgangspunten vastgelegd in bijlage 2) zoals bijvoorbeeld het bezoek aan niet-acceptabele internetsites of het versturen van onzedelijke e-mailberichten).

Artikel 2b – Wijze van monitoring elektronisch dataverkeer

Binnen ROC ASA wordt het elektronisch dataverkeer gemonitord volgens een protocol. Dit protocol is onlosmakelijk verbonden met dit reglement en is opgenomen als bijlage 2.

Artikel 3 – Verantwoordelijke, betrokken contactpersoon en bewerkers

- a Het College van Bestuur van de Regionale Opleidingen Centrum Amsterdam, 't-Sticht, Amersfoort is verantwoordelijk voor de gegevensverwerking.
- b Het hoofd van de afdeling ICT-beheer is de contactpersoon.
- c Indien voor de verwerking van persoonsgegevens derden worden ingezet (bewerkers volgens art. 1 lid e WBP), zullen deze door middel van expliciete bepalingen in de opdrachtverstrekking worden gebonden aan de Gedragscode en dit reglement.

Artikel 4– Categorieën van betrokkenen

De verwerking heeft betrekking op gegevens omtrent alle gebruikers van de beschikbare voorzieningen voor elektronisch dataverkeer, waaronder in ieder geval alle medewerkers, deelnemers en ex-deelnemers.

Artikel 5– Te verwerken gegevens

- a Gegevens inzake de aard en duur van het gebruik dat wordt gemaakt van elektronische gegevensuitwisseling;
- b Een administratienummer / log-in-naam, waarmee geen andere informatie te verkrijgen is dan welke waarop dit reglement van toepassing is;
- c Overige gegevens, voor zover deze naar mening van het College van Bestuur passen binnen het reglement. Indien het College dergelijke gegevens toe wenst te voegen aan de registratie, wordt dit vooraf schriftelijk kenbaar gemaakt, bijvoorbeeld door plaatsing in een schoolkrant. Bijlage 1 wordt per ingangsdatum van de registratie aangepast.

De gegevens zijn in detail weergegeven in bijlage 1 behorend bij dit reglement.

Artikel 6– Herkomst van gegevens

De in artikel 5, onder a tot met b, bedoelde gegevens worden onderscheidenlijk als volgt verkregen:

- a Geautomatiseerd.
- b Geautomatiseerd;
Betrokkene.

Artikel 7– Gegevensverstrekking aan categorieën van personen of instanties

De in artikel 5 bedoelde gegevens kunnen verstrekt worden aan:

- a Personen die sancties kunnen opleggen na ongeoorloofd gebruik (zoals vastgelegd in bijlage 2);
- b Justitie, in geval van (vermoedens van) strafbare gedragingen.

Artikel 8– Beveiliging van gegevensverwerking

Er dienen voldoende organisatorische, technische en fysieke maatregelen getroffen te zijn, zodat aan de wettelijke eisen inzake de beveiliging tegen verlies of tegen enige vorm van onrechtmatige verwerking wordt voldaan.

Artikel 9– Betrokken derde(n) bij gegevensverwerking

Op het moment van opstellen van dit reglement wordt personeel van derden ingezet voor het beheer van het Educatief Netwerk en het Administratief Netwerk: Human Informatics..

In overeenstemming met artikel 3, lid c van dit reglement zijn deze derden krachtens de opdrachtverstrekking d.d. 10-06-2002 gebonden aan dit reglement.

Artikel 10– Invoer, opnemingsduur wijziging en verwijdering van gegevens

- a Met het invoeren, wijzigen en verwijderen van gegevens zijn belast de in artikel 3 onder b bedoelde en de uit hoofde van hun functie daartoe aangewezen personen.
- b De in artikel 5 onder a t/m b bedoelde gegevens worden in beginsel bewaard gedurende drie werkdagen, tenzij sprake is van vermoedens van onjuist gebruik (zie bijlage 2). Dan geldt een termijn van één maand.
Gegevens op basis waarvan door daartoe bevoegde personen nadere actie is ondernomen, worden bewaard zolang dit met het oog op wettelijke bewaartermijnen, vanwege gerechtelijke en buitengerechtelijke procedures of in verband met organisatorische redenen in redelijkheid noodzakelijk is.
- c Bij onduidelijkheden in bewaartermijnen zal de verantwoordelijke een standpunt innemen.
- d Na het verstrijken van de opnemingsduur bedoeld in lid b, dan wel zoveel eerder als het doel van de registratie toelaat, kan bij verwijdering, al dan niet na een hiertoe strekkend verzoek van de geregistreerde zoals bedoeld in artikel 11 van dit reglement, worden besloten tot:
 - hetzij a. vernietiging van gegevens;
 - hetzij b. anonimiseren van gegevens;
 - hetzij c. opname in een andere registratie met een andere aangepaste doelstelling, met instemming van de geregistreerde, dan wel met kennisgeving aan de geregistreerde.

Artikel 11– Verzoek om kennisneming en verbetering, aanvulling en verwijdering van gegevens en om kennisneming van verstrekking van gegevens aan een derde

Iedere betrokkene kan een schriftelijk en rechtsgeldig ondertekend verzoek tot kennisneming,

verbetering, aanvulling, verwijdering en/of kennisneming indienen, met inachtneming van artikelen 13 en 14 van de gedragscode.

Artikel 12– Inzage reglement

- a Dit reglement, inclusief genoemde bijlagen, wordt ter inzage gelegd bij elk van de binnen het ROC-ASA onderkende vestiging.
- b Aan een ieder wordt op verzoek en tegen betaling van de kosten een exemplaar van dit reglement verstrekt.

Artikel 13– Slotclausule

In gevallen waarin dit reglement niet voorziet, zal de verantwoordelijke een standpunt innemen. In dergelijke gevallen zal het reglement en/of de bijlage(n) worden aangepast aan deze standpunten.

BIJLAGE 1

overzicht gegevens

- log-in nummer (administratienummer)
- log van bezochte pagina's
- tijdsduur Internetgebruik; al dan niet gespecificeerd per bezochte pagina
- log van gedownloade en ge-uploade bestanden (op naam en omvang)

- log van geadresseerden/afzenders van respectievelijk verstuurd/ontvangen e-mailberichten
- log van omvang van verstuurd en ontvangen e-mailberichten, al dan niet gespecificeerd per bericht
- log van verstuurd en ontvangen bijlagen ('attachements') naar naam en omvang

Bewaartermijnen

Zie bijlage 2 'procedures voor monitoring elektronisch dataverkeer'.

BIJLAGE 2

Procedures voor monitoring elektronisch dataverkeer

Protocol Internetgebruik

Toegang

1. Per locatie bepaalt de eindverantwoordelijke randvoorwaarden en vereisten om vast te stellen welke medewerkers toegang tot het Internet dienen te hebben.
2. Per locatie bepaalt de eindverantwoordelijke randvoorwaarden en vereisten om vast te stellen welke deelnemers toegang tot het Internet moeten hebben.
3. Per locatie stelt de eindverantwoordelijke vast welke hardware-matige beschermingen op de Internettoegang dienen te worden aangebracht (zoals –inhoudelijke- filters, beperking van omvang te down- / uploaden bestanden e.d.).
4. Per locatie stelt de eindverantwoordelijke vast voor welke opleidingen, momenten en PC's het gebruik van de filters tijdelijk wordt uitgeschakeld, alsmede hoe wordt omgegaan met verzoeken buiten die (initiële) vaststelling.

Ongewenst gebruik

5. Gebruik van Internet voor privédoeleinden is in beginsel met mate toegestaan. Voorwaarden hierbij zijn minimaal:
 - de werkzaamheden en/of studie-activiteiten leiden niet onder het privégebruik;
 - het privégebruik leidt niet tot overmatige belasting van het netwerk;
 - privégebruik vindt hoofdzakelijk plaats buiten de reguliere werktijden.Per locatie kan de eindverantwoordelijke nadere voorwaarden stellen en/of vanwege zwaarwegende redenen privégebruik geheel verbieden.
6. Het gebruik van Internet voor onzedelijke en/of onwettige doeleinden is niet toegestaan. Hierbij dient te worden gedacht aan *onder andere* het bezoeken van seksueel getinte websites (anders dan voor het werk noodzakelijk) en het down- / uploaden van illegale beeld- / muziekbestanden.

Toezicht

7. Aan de hand van geautomatiseerde logging van het Internetgebruik en analyse (zie punt 11) daarvan wordt toezicht gehouden op het naleven van dit protocol.
8. De logging bestaat uit registratie van de log-in-naam, datum en tijdstip met daarbij de bezochte Internetpagina's plus tijdsduur (per pagina), en een overzicht van gedownloade / ge-uploade bestanden naar naam en omvang.
9. Deze logging wordt in beginsel gedurende drie werkdagen bewaard. In geval van nader onderzoek (zie punten 10 en 11) kan de logging gedurende één maand worden bewaard. In geval van sancties en/of procedures, wordt de logging bewaard voor zolang dit wettelijk en/of redelijkerwijs noodzakelijk is.

10. Algemene bevindingen van de Afdeling ICT Beheer (bijvoorbeeld omtrent de prestaties van het netwerk) kunnen aanleiding zijn tot nader onderzoek naar het Internetgebruik. Hierover beslist de eindverantwoordelijke per locatie, na overleg met het hoofd ICT Beheer.
 11. Indien iemand vermoedens heeft van ongewenst gebruik door een medewerker of deelnemer, dient hij/zij deze vermoedens met argumentatie ter kennis van de eindverantwoordelijke van de locatie te brengen.
 12. Deze eindverantwoordelijke kan aan de Afdeling ICT Beheer opdracht geven tot nader onderzoek naar de logging van het Internetgebruik door de betrokkene waarop de vermoedens betrekking hebben.
 13. Dit nader onderzoek heeft in eerste instantie betrekking op de laatste drie werkdagen.
 - a. Indien dit onderzoek NIET leidt tot bevestiging van de vermoedens, wordt het onderzoek onverwijld gestaakt. De betrokkene wordt vervolgens in kennis gesteld van het uitgevoerde onderzoek en de uitkomst daarvan.
 - b. Indien dit onderzoek WEL leidt tot (gedeeltelijke) bevestiging van de vermoedens, wordt het onderzoek voortgezet. Hiertoe kunnen de logging-gegevens maximaal één maand worden bewaard, te beginnen vanaf de derde werkdag na de start van het onderzoek. De betrokkene wordt onverwijld in kennis gesteld van het uitgevoerde onderzoek met de uitkomsten daarvan, en van het voortzetten van het onderzoek.
 14. Op basis van de uitkomsten van het voortgezette onderzoek, kan de eindverantwoordelijke van de locatie besluiten tot sancties.
 - a. In geval van te omvangrijk privégebruik, kan de sanctie bestaan uit het opheffen van de toegang tot het Internet;
 - b. In geval van overtreding van wetten en/of de normen omtrent zedelijkheid, kan de sanctie bestaan uit het opheffen van de toegang tot het Internet plus eventuele aanvullende -al dan niet juridische- sancties (zoals ontslag / schorsing en rechtsvervolging). In dit geval overlegt de eindverantwoordelijke met het College van Bestuur van ROC ASA en worden eventueel juridische instanties betrokken bij het voorkomende geval.
 15. In geval van juridische stappen, wordt de logging als zijnde bewijsmateriaal overgedragen aan de bevoegde instantie. De bewaartermijn van de logging is vanaf dat moment te bepalen door die instantie.
-

Protocol E-mail-gebruik

Toegang

1. Per locatie bepaalt de eindverantwoordelijke randvoorwaarden en vereisten om vast te stellen welke medewerkers een e-mailadres toegekend dienen te hebben.
2. Per locatie bepaalt de eindverantwoordelijke randvoorwaarden en vereisten om vast te stellen welke deelnemers een e-mailadres toegekend moeten hebben.

3. Per locatie stelt de eindverantwoordelijke vast welke hardware-matige beschermingen op het e-mailgebruik dienen te worden aangebracht (zoals beperking van omvang van verstuurde en/of ontvangen berichten c.q. bijlagen e.d.).
4. Het gebruik van zogenaamde web-based e-mailprogramma's en -adressen wordt in dit protocol gelijk gesteld aan de door ROC ASA ter beschikking gestelde e-mailfaciliteiten.
5. Per locatie stelt de eindverantwoordelijke vast voor welke opleidingen, momenten en PC's het gebruik van de hardware-matige bescherming tijdelijk wordt uitgeschakeld, alsmede hoe wordt omgegaan met verzoeken buiten die (initiële) vaststelling.

Ongewenst gebruik

6. Gebruik van e-mail voor privédoeleinden is in beginsel met mate toegestaan. Voorwaarden hierbij zijn minimaal:
 - de werkzaamheden en/of studie-activiteiten leiden niet onder het privégebruik;
 - het privégebruik leidt niet tot overmatige belasting van het netwerk;
 - privégebruik vindt hoofdzakelijk plaats buiten de reguliere werktijden.Per locatie kan de eindverantwoordelijke nadere voorwaarden stellen en/of vanwege zwaarwegende redenen privégebruik geheel verbieden.
7. Het gebruik van e-mail voor onzedelijke en/of onwettige doeleinden is niet toegestaan. Hierbij dient te worden gedacht aan *onder andere* het versturen van seksueel getinte berichten en / of bestanden (anders dan voor het werk noodzakelijk).

Toezicht

8. Aan de hand van geautomatiseerde logging van het e-mailgebruik en analyse (zie punt 12) daarvan wordt toezicht gehouden op het naleven van dit protocol.
9. De logging bestaat uit registratie van de log-in-naam, naam geadresseerde / verzender, onderwerp, datum, tijdstip en omvang van alle berichten (zowel verstuurd als ontvangen), met daarbij eveneens de naam en omvang van eventuele bijlagen bij deze berichten.
10. Deze logging wordt in beginsel gedurende drie werkdagen bewaard. In geval van nader onderzoek (zie punten 11 en 12) kan de logging gedurende één maand worden bewaard. In geval van sancties en/of procedures, wordt de logging bewaard voor zolang dit wettelijk en/of redelijkerwijs noodzakelijk is.
11. Algemene bevindingen van de Afdeling ICT Beheer (bijvoorbeeld omtrent de prestaties van het netwerk) kunnen aanleiding zijn tot nader onderzoek naar het e-mailgebruik. Hierover beslist de eindverantwoordelijke per locatie, na overleg met het hoofd ICT Beheer.
12. Indien iemand vermoedens heeft van ongewenst gebruik door een medewerker of deelnemer, dient hij/zij deze vermoedens met argumentatie ter kennis van de eindverantwoordelijke van de locatie te brengen.
13. Deze eindverantwoordelijke kan aan de Afdeling ICT Beheer opdracht geven tot nader onderzoek naar de logging van het e-mailgebruik door de betrokkene waarop de vermoedens betrekking hebben.

14. Dit nader onderzoek heeft in eerste instantie betrekking op de laatste drie werkdagen.
 - a. Indien dit onderzoek NIET leidt tot bevestiging van de vermoedens, wordt het onderzoek onverwijld gestaakt. De betrokkene wordt vervolgens in kennis gesteld van het uitgevoerde onderzoek en de uitkomst daarvan.
 - b. Indien dit onderzoek WEL leidt tot (gedeeltelijke) bevestiging van de vermoedens, wordt het onderzoek voortgezet. Hiertoe kunnen de logging-gegevens maximaal één maand worden bewaard, te beginnen vanaf de derde werkdag na de start van het onderzoek. De betrokkene wordt onverwijld in kennis gesteld van het uitgevoerde onderzoek met de uitkomsten daarvan, en van het voortzetten van het onderzoek.

15. Op basis van de uitkomsten van het voortgezette onderzoek, kan de eindverantwoordelijke van de locatie besluiten tot sancties.
 - a. In geval van te omvangrijk privégebruik, kan de sanctie bestaan uit het opheffen van de toegang tot de e-mailfaciliteiten;
 - b. In geval van overtreding van wetten en/of de normen omtrent zedelijkheid, kan de sanctie bestaan uit het opheffen van de toegang tot de e-mailfaciliteiten plus eventuele aanvullende -al dan niet juridische- sancties (zoals ontslag / schorsing en rechtsvervolging). In dit geval overlegt de eindverantwoordelijke met het College van Bestuur van ROC ASA en worden eventueel juridische instanties betrokken bij het voorkomende geval.

16. In geval van juridische stappen, wordt de logging als zijnde bewijsmateriaal overgedragen aan de bevoegde instantie. De bewaartermijn van de logging is vanaf dat moment te bepalen door die instantie.