AFG
Building the Difference

Richtlijn inzake
- het gebruiken en monitoren van internet- en e-mailverkeer en telefoongesprekken; en
- de inzage van het gebruikersaccount van een medewerker

4 december 2014

Inhoudsopgave

AFG
Building the Difference

Inleidende bepalingen

Deze richtlijn bepaalt of en hoe medewerkers van groepsondernemingen van AFG Arbonia-Forster-Holding AG (hierna 'AFG') gebruik mogen maken van internet- en telefoondiensten. Deze richtlijn heeft ook tot doel medewerkers en AFG te beschermen bij het monitoren van deze diensten en bij het bekijken van een gebruikersaccount. Lokale voorschriften die voorzien in strengere bepalingen of die worden gebruikt bij de uitvoering van de richtlijn moeten worden nageleefd.

1. Gebruik van internet- en telefoondiensten

Indien voor medewerkers internet- (internet/e-mail) en telefoondiensten ter beschikking staan, zijn deze bedoeld voor zakelijke doeleinden en om hen in staat te stellen hun werk beter en/of efficiënter of professioneler uit te voeren.

Het hoofd van de BU[1] beslist, of het gebruik uitsluitend beperkt is tot zakelijke belangen.
Er mogen geen webpagina's met criminele, pornografische of racistische inhoud worden bezocht. Ook deelname aan overeenkomstige activiteiten (bijvoorbeeld door ideeën uit te wisselen via chats, e-mails, enz.) is verboden. Automatische filters kunnen worden gebruikt om de inhoud van bepaalde categorieën te blokkeren. Dit zijn pagina's met de volgende inhoud: pornografie, criminele activiteiten, extremistische inhoud, chat, drugs.

Om veiligheidsredenen worden alle e-mails en elke internettoegang inclusief alle downloads automatisch gecontroleerd op virussen en gevaarlijke inhoud en indien nodig geblokkeerd. Dit geldt ook voor versleutelde internetverbindingen (bijvoorbeeld internetbankieren). In ieder geval moeten e-mails van onbekende afzenders of e-mails die in het onderwerp verwijzen naar virussen onmiddellijk ongelezen worden verwijderd. In geen geval mogen e-mailbijlagen van onbekende afzenders worden geopend.

2. Monitoren van internet- en telefoondiensten

2.1 Logbestanden

De IT-afdeling logt alle internetactiviteiten. Inkomende en uitgaande telefoongesprekken worden gelogd. Loggen wordt gedefinieerd als het continu vastleggen van specifieke gegevens betreffende 'wie', 'wat', 'wanneer' en vindt bij AFG plaats op de volgende punten:

- internet (bezochte webpagina's, gebruiker, datum, tijdstip)
- e-mail (afzender, ontvanger, datum, tijdstip, onderwerp)
- inloggen in het systeem (gebruiker, datum, tijdstip)
- telefoon (telefoonnummers van alle abonnees, tijdstip, datum, duur)

2.2 Verbod op spyware

Er mag geen spyware worden gebruikt. Spyware zijn programma's waarmee medewerkers zonder hun medeweten kunnen worden gevolgd.

2.3 Evaluatie van de logbestanden

De logbestanden worden op verschillende niveaus geëvalueerd.

Anonieme evaluatie: Dit wordt gebruikt om statistieken te genereren, zoals de gestructureerde weergave van het gemiddelde internetgebruik, de meest bezochte websites, enz. Het aantal onderzochte personen moet

[1] De CEO beslist voor de medewerkers van AFG Management AG.

groot genoeg worden gehouden, zodat er geen conclusies kunnen worden getrokken over individuele medewerkers (bijv. alle medewerkers van AFG Management AG).

Persoonlijke evaluatie: Een persoonlijke evaluatie is alleen toegestaan als bij de anonieme evaluatie misbruik is geconstateerd of als er een ander vermoeden van misbruik bestaat. Elke schending van de gebruiksvoorwaarden in overeenstemming met artikel 1 van deze richtlijn of andere verplichtingen uit een arbeidsovereenkomst wordt beschouwd als misbruik.

De persoonlijke evaluatie vindt plaats op verzoek van de leidinggevende en wordt uitgevoerd door de verantwoordelijke HR-afdeling in samenwerking met de ICT-afdeling en, indien aanwezig, de functionaris voor gegevensbescherming. Indien een vermoeden van misbruik niet gegrond is, worden de persoonlijke evaluaties per direct stopgezet en worden de verzamelde gegevens vernietigd.

2.4 Monitoring als onderdeel van het waarborgen van de veiligheid en functionaliteit van het IT-systeem van het bedrijf

Mocht zich ondanks technische beveiligingsmaatregelen toch een storing in het IT-systeem voordoen, dan kunnen de logbestanden worden gebruikt om de oorzaak te achterhalen. Indien de oorzaak van de storing misbruik is, kan de geïdentificeerde medewerker worden gesanctioneerd volgens artikel 4 van deze richtlijn.

2.5 Bewaartermijn

De logbestanden van internetactiviteiten worden vier weken als bewijs bewaard, tenzij sancties of strafrechtelijke procedures een langere bewaartermijn vereisen. Het bewaren van de telefoonloggegevens is gebaseerd op de plaatselijk geldende bepalingen van het telecommunicatierecht.

3. Onderscheid tussen privé- en zakelijke e-mails

Het e-mailaccount wordt voornamelijk gebruikt voor zakelijke doeleinden. Beperk privécommunicatie tot een minimum. AFG monitort of verwerkt geen e-mails die als privé zijn gemarkeerd. Indien er geen onderscheid wordt gemaakt tussen privé- en zakelijke e-mails en het privé-karakter van een e-mail door de adresseringselementen niet kan worden geïdentificeerd of anderszins kan worden aangenomen, mag AFG ervan uitgaan dat de e-mail zakelijk is. Als er twijfels zijn over de aard van een e-mail, moet dit met de medewerker worden opgehelderd.

Naast de systeemback-up kunnen zakelijke e-mails desgewenst buiten de persoonlijke mailbox worden opgeslagen. .

Zodra wordt herkend dat een e-mail een privékarakter heeft, mag AFG geen kennis nemen van de inhoud ervan. Dit geldt ook als het vermoeden bestaat dat er per e-mail een strafbaar feit is gepleegd of als er sprake is van een ander geval van misbruik in overeenstemming met artikel 1 van deze richtlijn.

4. Sancties bij misbruik

Indien voldaan is aan de voorwaarden en regels voor monitoring en geconstateerd wordt dat er sprake is van misbruik, kunnen sancties op grond van het arbeidsrecht worden opgelegd (waarschuwing, blokkeren internettoegang, ontslag, enz.).

Voordat eventueel onrechtmatig verkregen bestanden worden verwijderd, wordt de betrokken medewerker geïnformeerd en, indien gerechtvaardigd, in de gelegenheid gesteld de betreffende bestanden (bijvoorbeeld privé e-mails) op een privé gegevensdrager op te slaan.

AFG
Building the Difference

5. E-mailbeheer bij afwezigheden/vertrekkende medewerkers

5.1 Geplande afwezigheid

Bij afwezigheid van een dag of meer moet een automatisch afwezigheidsbericht in Outlook geactiveerd worden. In het afwezigheidsbericht moet worden vermeld wie de plaatsvervanger is voor dringende zaken (inclusief contactgegevens) en of de inkomende e-mails automatisch worden doorgestuurd of niet. Alle e-mails naar de plaatsvervanger doorsturen, is slechts in uitzonderlijke gevallen toegelaten.

Als een medewerker per ongeluk vergeten is een afwezigheidsbericht te activeren, moet volgens artikel 6 te werk worden gegaan.

5.2 Onvoorziene afwezigheid

Bij onvoorziene afwezigheid (bijv. door ziekte, ongeval) zorgt de medewerker ervoor dat dringende, inkomende e-mails zo snel mogelijk worden doorgestuurd. Dit kan bijvoorbeeld door gebruik te maken van het betreffende beveiligde access portal. De medewerker kan ook een plaatsvervanger aanwijzen die bevoegd is om inkomende zakelijke e-mails te bekijken en zo nodig te verwerken. Als de medewerker er niet in slaagt de e-mails door te sturen, moet volgens artikel 6 te werk worden gegaan.

5.3 Onvoorziene langdurige afwezigheid

Indien bij onvoorziene afwezigheid de terugkeer naar het werk niet te voorzien is of de afwezigheid bijzonder lang duurt (meer dan 4 weken), kan (nadere) toegang worden geregeld volgens artikel 6.

5.4 Vertrek van een medewerker

De vertrekkende medewerker is verantwoordelijk voor het overhandigen van alle zakelijke documenten. Hij moet de schijven en de inbox opschonen voordat hij vertrekt. Alle lopende zaken zoals e-mails enz. of andere informatie die nodig of nuttig is voor AFG, moeten worden doorgestuurd. De vertrekkende medewerker moet ook een afwezigheidsbericht instellen, dat informeert dat het e-mailadres niet langer geldig is en dat de contactgegevens van de opvolger bevat.

De vertrekkende medewerker heeft de mogelijkheid om privé-e-mails en andere privédocumenten te verwijderen of op te slaan op een privégegevensdrager.

Het gebruikersaccount (inclusief e-mailaccount) wordt uiterlijk op de laatste effectieve werkdag geblokkeerd. Als het nodig is om het e-mail- of een gebruikersaccount te bekijken nadat deze is geblokkeerd, is het inzagerecht gebaseerd op artikel 6. Als het afwezigheidsbericht niet is ingesteld door de vertrekkende medewerker, moet volgens artikel 6 te werk worden gegaan en een afwezigheidsbericht worden geactiveerd. Er moet voor worden gezorgd dat er geen conclusies kunnen worden getrokken over de aard van de beëindiging van de arbeidsrelatie.

Het gebruikersaccount wordt uiterlijk 30 dagen na de laatste effectieve werkdag verwijderd. In uitzonderlijke gevallen wordt het gebruikersaccount uiterlijk 90 dagen na de laatste effectieve werkdag verwijderd.

5.5 Afwijkingen van artikelen 5.1 tot en met 5.4

Toegestane afwijkingen van artikelen 5.1 tot en met 5.4 zijn uiteengezet in bijlage 2.

6. Inzage van het gebruikersaccount van een medewerker

Indien inzage van het e-mailaccount van een medewerker toch noodzakelijk is ondanks wat in artikel 5 bepaald is, dient eerst contact op te worden genomen met de betreffende medewerker en dient zijn of haar toestemming voor inzage te worden verkregen. Indien deze de inzage weigert of niet bereikbaar is, moet de leidinggevende een schriftelijk verzoek indienen bij de verantwoordelijke HR-afdeling (zie bijlage). Goedkeuring wordt alleen verleend als AFG een hoger belang heeft (bijvoorbeeld dringende, operationele redenen), de terugkeer van de medewerker niet kan worden afgewacht en alle maatregelen zijn genomen om inzage te voorkomen. Het automatisch doorsturen van alle e-mails is alleen in uitzonderlijke gevallen toegestaan.

Als de aanvraag wordt goedgekeurd, wordt er een bericht gestuurd naar de IT-afdeling, die toegang tot het gebruikersaccount mogelijk maakt (door het wachtwoord opnieuw in te stellen of een koppeling te maken). De leidinggevende en een medewerker van de afdeling HR nemen deel aan de inzage (vier-ogen-principe). Uiterlijk op de dag dat hij weer aan het werk gaat, wordt de afwezige medewerker hierover geïnformeerd.

De inzage is qua tijd en inhoud beperkt tot de gegevens die in het aanvraagformulier werden verstrekt. Alleen zakelijke e-mails mogen worden bekeken. Als privé herkende e-mails mogen niet worden geopend, bekeken, verplaatst, gekopieerd, doorgestuurd en/of verwijderd (zie ook artikel 3). De leidinggevende stuurt de noodzakelijke e-mails naar zichzelf door. Daarnaast moet een afwezigheidsbericht worden geactiveerd, met de informatie met wie contact kan worden opgenomen voor dringende zaken.

Deze bepalingen gelden op dezelfde wijze nadat een medewerker het bedrijf heeft verlaten en voor de inzage in de gebruikersmap.

7. Vermoeden van crimineel gedrag

Als een strafbaar feit wordt vastgesteld of vermoed door de evaluatie van de logbestanden of andere aanwijzingen, worden de bijbehorende logbestanden bewaard. AFG behoudt zich het recht voor om strafrechtelijke vervolging in te stellen tegen de betrokkene. Indien inzage in privé e-mails, gegevens enz. noodzakelijk is, kan dit alleen met voorafgaande toestemming van de verdachte medewerker. Als het niet mogelijk is om deze vooraf te verkrijgen of als de toestemming wordt geweigerd, moet de zaak in het algemeen worden overgedragen aan de bevoegde wetshandhavingsinstantie. Bij uitzondering kan AFG zelf inzage verrichten, indien een hoger belang en specifieke vermoedens dit rechtvaardigen. De inzage is gebaseerd op artikel 6 hierboven.

AFG verbindt zich ertoe de resultaten van de onderzoeken vertrouwelijk te behandelen tegenover derden, in het bijzonder tegenover andere medewerkers.

8. Het gebruik van clouds

Clouds zijn virtuele IT-infrastructuren voor het opslaan van informatie op het internet (bijv. Dropbox). Het gebruik van clouds kan grote voordelen met zich meebrengen, omdat u bijvoorbeeld thuis of onderweg toegang heeft tot de gegevens die in de cloud zijn opgeslagen. Tegelijkertijd brengen clouds echter ook grote veiligheidsrisico's met zich mee. Om deze reden is het gebruik van een cloud alleen toegestaan als deze is goedgekeurd door het verantwoordelijke hoofd van de BU[2] na advies van de verantwoordelijke IT-afdeling.

[2] De CEO is verantwoordelijk voor de medewerkers van AFG Management AG.

AFG
Building the Difference

9. Afwijkingen

Afwijkingen van bovenstaande artikelen zijn alleen toegestaan na overleg met het hoofd van Legal & Compliance.

10. Informatie

Informatie in verband met onderhavige richtlijn kan worden verkregen bij het hoofd van Legal & Compliance.

11. Inwerkingtreding

Deze richtlijn treedt per direct in werking en vervangt de richtlijn betreffende het toezicht op en het gebruik van internet, e-mail en telefoon van 29 augustus 2013.

Arbon, 4 december 2014

AFG Arbonia-Forster-Holding AG

William J. Christensen	Andrea Wickart
Chief Executive Officer	Head of Legal & Compliance
	Algemene secretaresse

AFG
Building the Difference

Bijlage 1: Aanvraagformulier voor het recht op inzage in een gebruikersaccount van een medewerker

Betrokken medewerker	
Naam:	Bedrijf:
Functie:	
Voorwerp van de inzage	
□ E-mails	□ Bestanden
Reden van de inzage	
□ geplande afwezigheid	geplande datum van terugkeer:
□ onvoorziene afwezigheid	
□ Medewerker heeft het bedrijf al verlaten	Vertrek op:
□ Vermoeden van crimineel gedrag	Specifieke gronden voor vermoeden:
De inzage is dringend nodig, omdat	
Omvang van de inzage (zo gedetailleerd mogelijk)	
E-mails of bestanden over de volgende onderwerpen zijn dringend nodig:	Er moet naar e-mails of bestanden uit de volgende periode worden gezocht:
Contact met de betrokken medewerker	
□ Ja, er is geprobeerd vooraf toestemming van de betrokken medewerker te verkrijgen, met als resultaat:	□ Nee, er is niet geprobeerd vooraf toestemming van de betrokken medewerker te verkrijgen, omdat:
Alternatieven	
Het volgende is gedaan om inzage te voorkomen:	
□ de benodigde bestanden zijn gezocht in de gemeenschappelijke map (schijf G: / gemeenschappelijk e-mailaccount).	□ de vereiste bestanden/e-mails werden van andere teamleden van de afwezige gevraagd.
□ Overige:	
Plaats / Datum	**Handtekening**

AFG
Building the Difference

Bijlage 2: Afwijkingen van de artikelen 5.1 tot en met 5.4 van de richtlijn inzake het monitoren en gebruiken van internet, e-mail en telefoon

Om operationele en technische redenen gelden de volgende afwijkingen van de artikelen 5.1 tot en met 5.4 voor de divisie Gebouwentechniek:

Instellen van een afwezigheidsbericht
Binnen de divisie Gebouwentechniek worden in principe geen afwezigheidsberichten ingesteld. De betrokken medewerkers wordt opgedragen bij geplande of onvoorzienbare afwezigheden en bij vertrek

(a) een plaatsvervanger aan te wijzen die bevoegd is om inkomende zakelijke e-mails te bekijken en zo nodig te verwerken; of
(b) het automatisch doorsturen van alle inkomende e-mails in te stellen.

Het aanwijzen van de plaatsvervanger of het instellen van een automatische doorschakeling kan alleen door de medewerker zelf gedaan worden.

Verwijdering van het gebruikersaccount wanneer een medewerker vertrekt
Het gebruikersaccount wordt meestal 30 dagen na de laatste effectieve werkdag verwijderd, maar ten vroegste wanneer de opzegtermijn is verstreken. In uitzonderlijke gevallen kan de verwijdering op een later tijdstip plaatsvinden, maar uiterlijk wanneer de bedrijfsdoelstellingen zijn bereikt.