AFG
Building the Difference

Política relativa
- à utilização e controlo do tráfego de Internet e de e-mail e chamadas telefónicas; assim como
- à inspeção da conta de utilizador de um colaborador

04 de dezembro de 2014

AFG
Building the Difference

Índice

AFG
Building the Difference

Preâmbulo

A presente política explica se e como os colaboradoress das empresas do grupo AFG Arbonia-Forster-Holding AG (doravante "AFG") devem utilizar os serviços de Internet e serviços de telefone. Além disso, o objetivo desta política é proteger os colaboradores e a AFG ao controlar estes serviços e ao inspecionar uma conta de utilizador. Os regulamentos locais que prevêem disposições mais rigorosas ou que são aplicados na implementação da política devem ser observados.

1. Utilização de serviços de Internet e serviços de telefone

Se os serviços de Internet (Internet/e-mail) e serviços telefónicos estiverem disponíveis para os colaboradores, estes destinam-se a fins profissionais e destinam-se a permitir que o trabalho seja realizado de forma mais eficiente e/ou profissional.

O Chefe da BU[1] decide se a utilização abrange exclusivamente assuntos relacionados à empresa.
Nenhuma página web com conteúdo criminoso, pornográfico e racista pode ser pesquisada. Igualmente, é proibida a participação nas atividades indicadas (por exemplo, troca de opiniões através de chats, e-mails, etc.). Filtros automáticos podem ser utilizados para bloquear o conteúdo de certas categorias. Tratam-se de páginas com o seguinte conteúdo: pornografia, atividades criminosas, conteúdo extremista, chat, drogas.

Por motivos de segurança, todos os e-mails e acessos à internet, incluindo downloads, são verificados quanto a vírus e conteúdo prejudicial e, caso necessário, bloqueados. O mesmo se aplica a ligações encriptadas na Internet (por exemplo, Internet Banking). No entanto, os e-mails de remetentes desconhecidos ou aqueles que apresentem vírus no assunto devem ser imediatamente apagados sem serem lidos. Em nenhuma circunstância devem ser abertos os anexos de e-mails de remetentes desconhecidos.

2. Controlo de serviços de Internet e serviços de telefone

2.1 Registos

O Departamento de Informática regista as atividades na Internet. As chamadas telefónicas recebidas e efetuadas são registadas. Um registo é definido como a gravação contínua de dados marginais "quem", "o quê", "quando" e tem lugar na AFG nos seguintes locais:

- Internet (páginas da Internet pesquisadas, utilizador, data, hora)
- E-mail (remetente, destinatário, data, hora, linha de assunto)
- Início de sessão no sistema (utilizador, data, hora)
- Telefone (número de telefone de todos os participantes, hora, data, duração)

2.2 Proibição de programas espiões

Nenhum programa espião (denominado spyware) pode ser utilizado. É entendido como programa espião, todos os programas que permitem o controlo de colaboradores sem o seu conhecimento.

2.3 Avaliação dos registos

A avaliação dos protocolos é feita em diferentes níveis.

Avaliação anónima: Serve para a elaboração de estatísticas como, por exemplo, a representação estruturada da utilização média da Internet, as páginas web mais frequentemente visitadas, etc.. A quantidade de pessoas

[1] Para os colaboradores da AFG Management AG, o CEO toma as decisões.

controladas deve ser suficientemente grande, para que não seja possível identificar colaboradores concretos (por exemplo, todos os colaboradores da AFG Management AG).

Avaliação pessoal: A avaliação pessoal só é permitida se tiver sido detetada uma utilização indevida pela avaliação anónima ou se existir, de outra forma, uma suspeita de utilização indevida. Como utilização indevida considera-se qualquer violação das disposições de utilização da alínea 1 da presente política ou de outras obrigações decorrentes do contrato de trabalho.

A avaliação pessoal é realizada a pedido do supervisor e é realizada pelo Departamento de Recursos Humanos responsável, em cooperação com o Departamento de Informática e, se disponível, com o encarregado pela proteção de dados. Se uma suspeita de utilização indevida não for fundamentada, as avaliações pessoais são imediatamente interrompidas e os dados recolhidos eliminados.

2.4 Controlo no contexto de garantia de segurança e operabilidade do sistema informático da empresa

Se ocorrer uma falha no sistema informático, apesar das medidas técnicas de proteção, os registos podem ser consultados na procura da sua causa. Se a causa da falha for uma utilização indevida, o colaborador identificado pode ser sancionado de acordo com a alínea 4 da presente política.

2.5 Duração do armazenamento

Para efeitos de preservação de provas, os registos das atividades na Internet são mantidos por quatro semanas, a menos que qualquer processo de sanção ou criminal torne necessário um armazenamento mais longo. O armazenamento de registos telefónicos é determinado pelas disposições localmente aplicáveis da lei de telecomunicações.

3. Distinção entre e-mails privados e profissionais

A conta de e-mail é utilizada principalmente para fins profissionais. Comunicações privadas devem ser limitadas para um mínimo. A AFG não inspeciona nem processa e-mails que são marcados como privados. Se não houver distinção entre e-mails privados e empresariais e se a natureza privada de um e-mail não poder ser reconhecida ou não puder ser assumida com base nos elementos de endereçamento, a AFG pode assumir que o e-mail é profissional. Se existirem dúvidas sobre a natureza de um e-mail, estas devem ser clarificadas com o colaborador.

Para além da cópia de segurança do sistema, os e-mails profissionais podem ser guardados fora da caixa de entrada pessoal, se necessário. .

Assim que for reconhecido que um e-mail é de natureza privada, a AFG pode não tomar conhecimento do seu conteúdo. Isto aplica-se mesmo que se suspeite que foi cometido um delito por meio de e-mail ou se houver qualquer outro caso de utilização indevida de acordo com a alínea 1 da presente política.

4. Sanções em caso de utilização indevida

Se os requisitos e regras de controlo tiverem sido cumpridas e se se tiver tornado evidente que ocorreu uma utilização indevida, poderão ser impostas sanções ao abrigo da legislação laboral (aviso, bloqueio de acesso à Internet, despedimento, etc.).

Antes de os ficheiros adquiridos invedidamente serem apagados, o colaborador afetado é informado e, se razoável, é-lhe dada a oportunidade de guardar os ficheiros em questão (por exemplo, e-mails privados) num suporte de dados privado.

5. Gestão de e-mails em caso de ausências/demissões de colaboradores

5.1 Ausência prevista

Para ausências de um dia ou mais, o Assistente Fora do Escritório deve ser ativado no Outlook. A notificação de ausência deve indicar quem é o/a representante para assuntos urgentes (incluindo detalhes de contacto) e se os e-mails recebidos são ou não são automaticamente encaminhados. O encaminhamento automático de todos os e-mails ao/à representante só deve ocorrer em circunstâncias excecionais.

Se um colaborador tiver inadvertidamente esquecido de ativar o Assistente Fora do Escritório, proceder como descrito na alínea 6.

5.2 Ausência imprevista

Em caso de ausência imprevista (como doença, acidente), o colaborador deve assegurar o mais rapidamente possível de que os e-mails recebidos urgentes sejam encaminhados. Isto pode ser feito, por exemplo, através do respetivo portal de acesso seguro. O colaborador pode também designar um/uma representante que está autorizado/autorizada a visualizar e, se necessário, a processar os e-mails profissionais recebidos. Se o colaborador não estiver em condições de assegurar o encaminhamento dos e-mails, proceder como estabelecido na alínea 6.

5.3 Ausência imprevista de longa duração

Se, em casos de ausência imprevista, o regresso ao local de trabalho não for previsível ou se a ausência for particularmente longa (mais de 4 semanas), (mais) inspeções podem ser realizadas de acordo com a alínea 6.

5.4 Demissão de um colaborador

O colaborador demitido é responsável pela entrega de todos os documentos empresariais. O mesmo tem de limpar as unidades de disco e a caixa de entrada antes da sua saída. Quaisquer assuntos pendentes, tais como e-mails, etc., ou outras informações necessárias ou úteis à AFG, serão encaminhados. O colaborador demitido deve também configurar o Assistente Fora do Escritório, que informa que o e-mail já não é válido e que contém os dados de contacto do substituto.

O colaborador demitido tem a opção de apagar e-mails privados e outros documentos privados ou de os guardar num suporte de dados privado.

A conta de utilizador (incluindo a conta de e-mail) será bloqueada, o mais tardar, no último dia de trabalho efetivo. Se for necessário inspecionar a conta de e-mail ou uma pasta de utilizador depois de esta ter sido bloqueada, o direito de inspeção é determinado pela alínea 6. Se o Assistente Fora do Escritório não tiver sido configurado pelo colaborador demitido, proceder como estabelecido na alínea 6 e ativar o Assistente Fora do Escritório. Deve ter-se o cuidado de assegurar que não se possam tirar conclusões quanto à natureza da cessação da relação laboral.

A conta de utilizador será eliminada, o mais tardar, 30 dias após o último dia de trabalho efetivo. Em casos excecionais, a conta de utilizador será eliminada, o mais tardar, 90 dias após o último dia de trabalho efetivo.

5.5 Divergências das alíneas 5.1 a 5.4

As divergências permitidas das alíneas 5.1 a 5.4 são estabelecidas no Anexo 2.

6. Inspeção da conta de utilizador de colaboradores

Se, apesar das disposições da alínea 5, for necessário inspecionar a conta de e-mail de um colaborador, o colaborador afetado deve ser primeiro contactado e o seu consentimento para a inspeção deve ser obtido. Se este recusar a inspeção ou se não puder ser contactado, o supervisor deve apresentar um requerimento por escrito ao Departamento de Recursos Humanos competente (cf. Anexo). A autorização só será concedida se a AFG tiver um interesse primordial (por exemplo, razões urgentes e profissionais), não for possível aguardar pelo regresso do colaborador e tiverem sido tomadas todas as medidas para impedir a inspeção. Um encaminhamento automático de todos os e-mails só é permitido em circunstâncias excecionais.

Se o requerimento for aprovado, tal é comunicado ao Departamento de Informática, que permite o acesso à conta do utilizador (redefinindo a palavra-passe ou criando uma ligação). O supervisor e um membro do Departamento de Recursos Humanos participam na inspeção (princípio dos quatro olhos). O empregado ausente será informado da situação, o mais tardar, no dia em que regressar ao trabalho.

A inspecão é limitada no tempo e no conteúdo às informações fornecidas no formulário de requerimento. Apenas devem ser visualizados e-mails profissionais. Os e-mails identificados como privados não podem ser abertos, vistos, movidos, copiados, encaminhados e/ou eliminados (cf. também a alínea 3). O supervisor encaminha a si próprio os e-mails necessários. Além disso, o Assistência Fora do Escritório deve ser ativado com a indicação de quem deve ser contactado para assuntos urgentes.

Estas disposições aplicam-se de forma análoga após a demissão de um colaborador e para a inspeção em pastas do utilizador.

7. Suspeita de um comportamento punível

Se um delito for determinado ou suspeito através da avaliação dos registos ou através de outras indicações, os registos correspondentes são guardados. A AFG reserva-se o direito de apresentar queixa criminal contra a pessoa afetada. Se for necessário inspecionar e-mails, dados, etc. privados, tal só deve ser feito com o consentimento prévio do colaborador suspeito. Se a recolha prévia não for possível ou se consentimento for recusado, a questão deve, em princípio, ser remetida para a autoridade competente de aplicação da lei. Em casos excecionais, a AFG pode efetuar a inspeção se tal se justificar por interesse superior e por motivos de suspeita concreta. A inspeção é determinada pela alínea 6 acima referida.

A AFG compromete-se a tratar confidencialmente os resultados das investigações em relação a terceiros, especialmente também em relação a outros colaboradores.

8. A utilização de serviços cloud

Clouds são infraestruturas informáticas virtuais que guardam informação na Internet (por exemplo, Dropbox). A utilização de serviços cloud pode ter grandes vantagens, por exemplo, pode-se aceder aos dados guardados no serviço cloud a partir de casa ou durante uma viagem. Paralelamente, os serviços cloud apresentam grandes riscos de segurança. Por este motivo, a utilização de um serviço cloud só é permitida quando for autorizada

pelo Chefe da BU[2] responsável, após a obtenção de uma recomendação do Departamento de Informática responsável.

9. Divergências

Só serão admitidas divergências das alíneas acima referidas após conciliação com o Head of Legal & Compliance.

10. Informações

As informações relacionadas com a presente política serão fornecidas pelo Head of Legal & Compliance.

11. Entrada em vigor

Esta política entra em vigor imediatamente e substitui a política relativa ao controlo e utilização da Internet, e-mail e telefone de 29 de agosto de 2013.

Arbon, 04 de dezembro de 2014

AFG Arbonia-Forster-Holding AG

William J. Christensen	Andrea Wickart
Chief Executive Officer	Head of Legal & Compliance Secretária geral

[2] Para os colaboradores da AFG Management AG, o CEO é o responsável.

AFG
Building the Difference

Anexo 1: Formulário de requerimento para o direito de inspeção de uma conta de utilizador de um colaborador

Colaborador afetado	
Nome:	Empresa:
Função:	
Objeto da inspeção	
□ E-mails	□ Ficheiros
Motivo da inspeção	
□ Ausência prevista	retorno previsto em:
□ Ausência imprevista	
□ O funcionário já foi demitido	Demissão em:
□ Suspeita de um comportamento punível	Suspeita concreta:
A inspeção é urgentemente necessária porque	
Âmbito da inspeção (o mais detalhado possível)	
Os e-mails ou ficheiros sobre os seguintes tópicos são urgentemente necessários:	Devem-se procurar e-mails ou ficheiros dentro do seguinte período de tempo:
Contacto com o colaborador afetado	
□ Sim, foi feita uma tentativa de obter o consentimento prévio do colaborador afetado, com o seguinte resultado:	□ Não, não foi feita uma tentativa de obter o consentimento prévio do colaborador afetado, porque:
Alternativas	
O seguinte foi feito para evitar a inspeção:	
□ Os ficheiros necessários foram pesquisados na pasta partilhada (unidade de disco G:/conta de e-mail partilhada).	□ Os ficheiros/e-mails necessários foram solicitados a outros membros da equipa do colaborador ausente.
□ Outro:	
Local/Data	**Assinatura**

AFG
Building the Difference

Anexo 2: Divergências das alíneas 5.1 a 5.4 da política relativa ao controlo e utilização da Internet, e-mail e telefone

Por razões empresariais e técnicas, as seguintes divergências das alíneas 5.1 a 5.4 aplicam-se à Divisão de Tecnologia de Construção:

Configuração do Assistente Fora do Escritório
Por princípio, o Assistente Fora do Escritório não é configurado a nível externo na Divisão de Tecnologia de Construção. Os colaboradores afetados são instruídos, em caso de ausências previsíveis ou imprevisíveis, bem como em caso de demissão,

(a) a designar um/uma representante que está autorizado/autorizada a visualizar e, se necessário, a processar os e-mails profissionais recebidos; ou
(b) a estabelecer o encaminhamento automático de todos os e-mails recebidos.

A designação do/da representante ou a configuração do encaminhamento automático deve ser apenas realizado pelo colaborador.

Eliminação da conta de utilizador em caso de demissão de um colaborador
A conta de utilizador é geralmente eliminada 30 dias após o último dia de trabalho efetivo, mas não antes do fim do prazo de aviso prévio. Em casos excecionais, a eliminação pode ser feita numa data posterior, mas, o mais tardar, quando o fim empresarial tiver sido executado.