DATENSCHUTZKONFERENZ

Konferenz der unabhängigen
Datenschutzbehörden
des Bundes und der Länder

Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Die Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten der Nutzung des betrieblichen Internet- und E-Mail-Dienstes durch die Beschäftigten auf. Sie soll es den Arbeitgebern und den Beschäftigten erleichtern, eine klare Regelung im Unternehmen zu erreichen, soweit eine private Nutzung des Internets und/oder des E-Mail-Dienstes erlaubt sein soll. Zudem enthält diese Orientierungshilfe ein Muster für eine Betriebsvereinbarung/Richtlinie/Anweisung für die private Nutzung von Internet und/oder des betrieblichen E-Mail Postfachs.

Redaktionelle Bearbeitung:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach

E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de
Tel.: 0981/53-1300
Fax: 0981/53-5300

Stand:
Januar 2016

Inhaltsverzeichnis

A. Allgemeines

I. Überblick

„Darf ich am Arbeitsplatz privat das Internet nutzen? Darf ich am Arbeitsplatz private E-Mails versenden?“ – diese Fragen haben viele Beschäftigte, die Zugang zum Internet haben.

Für den Arbeitgeber stellen sich ähnliche Fragen: *„Darf ich auf das E-Mail-Postfach der Beschäftigten zugreifen, wenn sie ungeplant abwesend sind? Darf ich die Internetnutzung kontrollieren? Welche Gestaltungsmöglichkeiten habe ich im Voraus?“*

Datenschutzrechtlich bedeutsam sind in diesem Zusammenhang die anfallenden personenbezogenen Daten, und zwar sowohl der Beschäftigten als auch ihrer Kommunikationspartner und anderer Betroffener (z.B. Dritter, deren Namen in einer E-Mail genannt wird).

Für die Beurteilung der datenschutzrechtlichen Zulässigkeit der E-Mail- und Internetnutzung am Arbeitsplatz ist es sehr relevant, ob den Beschäftigten auch die private Nutzung des Internets und/oder des betrieblichen E-Mail-Postfachs am Arbeitsplatz gestattet worden ist.

Diese Orientierungshilfe stellt einige der hierbei zu beachtenden datenschutzrechtlichen Anforderungen dar und zeigt Regelungsmöglichkeiten auf. Sie richtet sich an die Wirtschaft und kann in der Regel entsprechend für den öffentlichen Dienst angewendet werden. Landesspezifische Vorschriften sind zu beachten.

Im Anhang befindet sich das Muster einer Betriebsvereinbarung und ergänzender Einwilligung, mit der die private Internet- und E-Mail-Nutzung geregelt werden kann. Das Muster kann auch als Beispiel genommen werden, um diese Punkte in eine Anweisung/Richtlinie oder in den einzelnen Arbeitsvertrag aufzunehmen.[1] Dies bietet sich insbesondere dann an, wenn es im Unternehmen keinen Betriebsrat gibt. Das Muster ist an die konkreten Gegebenheiten im jeweiligen Unternehmen anzupassen; zudem sind jeweils arbeitsrechtliche Fragestellungen zu beachten, die dieses Papier nicht erschöpfend berücksichtigen kann

[1] Aus Gründen der Übersichtlichkeit wird im Folgenden ausschließlich von der Betriebsvereinbarung gesprochen. Gemeint sind jedoch auch die Anweisung/Richtlinie oder eine Regelung im Arbeitsvertrag.

II. Rechtlicher Rahmen

1. Grundsatz

Soweit der Arbeitgeber Hardware bzw. Software zur Verfügung stellt, dürfen die betrieblichen Internet- und E-Mail-Dienste grundsätzlich nur für die betriebliche Tätigkeit genutzt werden. Eine private Nutzung von Internet und/oder betrieblichem E-Mail-Postfach ist daher nicht erlaubt, es sei denn, der Arbeitgeber hat eine Privatnutzung ausdrücklich z.B. im Arbeitsvertrag oder in einer Betriebsvereinbarung geregelt oder, was überwiegend als möglich angesehen wird, in Kenntnis und Duldung der privaten Nutzung über einen längeren Zeitraum (sog. „betriebliche Übung“) konkludent genehmigt.

Dem Arbeitgeber steht es frei, ob er eine Privatnutzung des Internets und/oder des betrieblichen E-Mail-Accounts erlaubt.

2. Gesetzlicher Rahmen

a) BDSG und Arbeitsrecht

Soweit die Nutzung des Internets und/oder des betrieblichen E-Mail-Postfachs ausschließlich zu betrieblichen Zwecken erlaubt ist, richtet sich die Erhebung, Verarbeitung und Nutzung von anfallenden personenbezogenen Daten nach dem Bundesdatenschutzgesetz (BDSG).

Da sich das öffentlich-rechtliche Datenschutzrecht gemäß BDSG, welches Gegenstand dieser Orientierungshilfe ist, und das zivilrechtliche Arbeitsrecht „überlappen“, sind parallel arbeitsrechtliche Fragestellungen zu berücksichtigen.

b) TKG und TMG

Wenn der Arbeitgeber den Beschäftigten auch die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfaches erlaubt, ist zusätzlich das Telekommunikationsgesetz (TKG) bzw. das Telemediengesetz (TMG) zu beachten. Nach Auffassung der Aufsichtsbehörden ist der Arbeitgeber in diesem Fall Telekommunikationsdienste- bzw. Telemediendienste-Anbieter. Dies hat die Konsequenz, dass er an das Fernmeldegeheimnis des § 88 Abs. 2 S. 1 TKG gebunden ist und gemäß § 11 Abs. 1 Nr. 1 TMG den Datenschutzvorschriften des TMG unterliegt. Zugleich bedeutet dies, dass sich der Arbeitgeber bei einer Verletzung des Fernmeldegeheimnisses gemäß § 206 Strafgesetzbuch (StGB) strafbar machen kann.

Zum rechtlichen Hintergrund: Das Fernmeldegeheimnis kann sich auch auf E-Mails erstrecken, die auf einem Server des jeweiligen Diensteanbieters zwischen- oder endgespeichert sind. Daher wird auch der „ruhende“ E-Mail-Verkehr erfasst, bei dem ein „dynamischer“ Telekommunikationsvorgang nicht (mehr) stattfindet (BVerfG, 16.6.2009, 2 BVR 902/06).

Solange also E-Mails im Herrschaftsbereich des jeweiligen Diensteanbieters verbleiben, folgt die Schutzbedürftigkeit der Kommunikationspartner aus dieser Einschaltung eines Dritten.

Einige Gerichte vertreten demgegenüber die Auffassung, dass Arbeitgeber, die die private Nutzung des Internets und/oder eines betrieblichen E-Mail-Postfachs gestatten oder dulden, nicht als Diensteanbieter im Sinne des TKG bzw. TMG anzusehen sind und daher nicht dem Fernmeldegeheimnis unterliegen. [2]

Solange jedoch diese Frage nicht höchstrichterlich oder durch den Gesetzgeber eindeutig geklärt ist, sollten Arbeitgeber zur Vermeidung etwaiger Strafbarkeit davon ausgehen, Diensteanbieter zu sein. Hiervon geht auch die vorliegende Orientierungshilfe aus.

Auf die Verpflichtung des Arbeitgebers, die Beschäftigten über die Erstellung von Einzelverbindungsnachweisen und deren Kenntnisnahme gem. § 99 Abs. 1 Satz 4 TKG zu informieren, wird hingewiesen.

B. Ausschließlich betriebliche Nutzung

I. Internet

1. Der Arbeitgeber hat grundsätzlich das Recht, anhand von Protokolldaten stichprobenartig[3] zu prüfen, ob das Surfen der Beschäftigten betrieblicher Natur ist. Dazu ist es in einem ersten Schritt zulässig und ausreichend, wenn sie für diesen Zweck zunächst nur eine Auswertung des Surfverhaltens ohne Personenbezug vornehmen, d.h. insbesondere auch ohne Einbeziehung der IP-Adresse und anderer Daten zur Identifizierung der einzelnen Beschäftigten. Grundsätzlich ist datenschutzfreundlichen Maßnahmen zur Begrenzung der Internetnutzung – z. B. Nutzung von black- und/oder whitelists – der Vorzug zu geben. Für die Erstellung solcher black- bzw. whitelists können hinsichtlich der Internetnutzung wirksam anonymisierte Protokolldaten herangezogen werden. Eine personenbezogene Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten unter den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG bei konkretem Missbrauchsverdacht im verhältnismäßi-

[2] Siehe: Hessischer VGH, 19.5.2009, AZ: 6 A 2672/08.Z; LAG Niedersachsen, 31.5.2010, AZ: 12 Sa 875/09; LAG Berlin-Brandenburg, 16.2.2011, AZ: 4 Sa 2132/10; VG Karlsruhe, 27.5.2013, AZ: 2 K 3249/12; VGH Baden-Württemberg, 30.7.2014, 1 S 1352/2013. Die genannten Gerichte haben zudem zum Teil die Auffassung vertreten, dass der Schutz des Fernmeldegeheimnisses jedenfalls in dem Moment endet, in dem der Empfänger in der Weise Zugriff auf die E-Mails in seinem betrieblichen E-Mail Postfach hat, dass er entscheiden kann, ob er sie im zentralen Posteingang belässt oder auf einen lokalen Rechner verschiebt/löscht.

[3] Zum Umfang von Stichproben wird auf die arbeitsrechtliche Rechtsprechung, insbesondere BAG, Beschluss vom 9.7.2013 - 1 ABR 2/13 (A) verwiesen.

gen Rahmen zulässig. Danach können zur Aufdeckung von Straftaten personenbezogene Daten der Beschäftigten erhoben, verarbeitet oder genutzt werden, wenn folgende Voraussetzungen vorliegen: Es müssen zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Betroffenen im Beschäftigungsverhältnis eine Straftat begangen haben. Zudem muss die Maßnahme zur Aufdeckung erforderlich sein. Letztlich darf nicht das schutzwürdige Interesse der Betroffenen überwiegen; insbesondere dürfen Art und Ausmaß nicht unverhältnismäßig sein.

2. Soweit im Zusammenhang mit der Nutzung des Internets personenbezogene Daten ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren gespeichert werden, dürfen diese Daten auch nur zu diesen Zwecken genutzt werden (§ 31 BDSG). Eine Nutzung dieser Daten zur Verhaltens- und Leistungskontrolle der Beschäftigten ist nicht erlaubt.

II. Nutzung des betrieblichen E-Mail-Accounts

1. Ein- und ausgehende betriebliche E-Mails der Beschäftigten darf der Arbeitgeber zur Kenntnis nehmen. Beispielsweise kann er verfügen, dass die Beschäftigten ihm jede für den Geschäftsgang relevante oder fest definierte ein- oder ausgehende E-Mail einzeln zur Kenntnis zuleiten. Eine durch den Arbeitgeber eingerichtete automatisierte Weiterleitung aller ein- und ausgehenden E-Mails an einzelne Vorgesetzte ist, sofern arbeitsrechtlich nicht statthaft, auch datenschutzrechtlich mangels Erforderlichkeit unzulässig (Verbot der permanenten Kontrolle).

2. Für den Fall der Abwesenheit kann eine Weiterleitung der E-Mail in Betracht kommen. Allerdings sollte im Hinblick auf die schutzwürdigen Belange der Beschäftigten die Verwendung eines Abwesenheitsassistenten vorgezogen werden. Aufgrund der schutzwürdigen Belange der Beschäftigten stellt dieses Vorgehen das mildeste Mittel dar. Nur wenn eine Abwesenheitsmitteilung nicht ausreicht, kann eine Weiterleitung in Betracht gezogen werden.

Auf bereits empfangene bzw. versandte betriebliche E-Mails darf der Arbeitgeber nur zugreifen, wenn dies für betriebliche Zwecke erforderlich ist.

3. E-Mails dürfen von dem Arbeitgeber nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter erkannt wurde. Etwas anderes kann im Falle erforderlicher Maßnahmen der Missbrauchskontrolle gelten.

4. a) Zur Missbrauchskontrolle gelten die Ausführungen zu B I 1 entsprechend.
b) Zur Regelung des § 31 BDSG (besondere Zweckbindung erhobener Daten) gelten die Ausführungen zu B I 2 entsprechend.

C. Private Nutzung

I. Internet

1. Ist die private Nutzung des Internets erlaubt (oder gilt sie als erlaubt, s.o. [4]), wird der Arbeitgeber hinsichtlich der privaten Nutzung zum Diensteanbieter im Sinne des TKG und unterliegt den Datenschutzbestimmungen des TMG. Er ist daher grundsätzlich zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen (Protokolldaten), ist dem Arbeitgeber nur mit Einwilligung der betreffenden Beschäftigten erlaubt. Dies betrifft insbesondere die Daten, aus denen sich ergibt, welche Internetseiten welche Beschäftigten wann aufgerufen haben. Ausnahmen gelten allerdings gemäß §§ 88 Abs. 3, 91 ff. TKG (z.B. erforderliche Maßnahmen zum Schutz der technischen Systeme, d.h. zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen).

2. Der Arbeitgeber kann die Erlaubnis einer Privatnutzung an Bedingungen knüpfen: Es bieten sich insbesondere Regelungen zum zeitlichen Umfang der Privatnutzung an. Auch konkrete Verhaltensregeln sollten vor Beginn der privaten Nutzung getroffen werden. Der Arbeitgeber braucht in diesem Zusammenhang eine Einwilligung der Beschäftigten, die sich darauf bezieht, dass diese mit Zugriffen des Arbeitgebers (wie unter 1. beschrieben) einverstanden sind. Die Einwilligung erstreckt sich also auf Art und Umfang von Zugriffen und Kontrollen. Diese Kontrollen umfassen die Einhaltung der Nutzungsregelungen (zeitlicher Umfang bzw. Inhalt der Nutzung).

3. Zur Einwilligung: Auf der „ersten Stufe“ sollte eine Betriebsvereinbarung abgeschlossen werden. In dieser sollte der Gegenstand der späteren, individuellen Einwilligungen umrissen werden. Sodann sind auf dieser Grundlage die individuellen Einwilligungen der einzelnen Beschäftigten einzuholen.

Die Einwilligung sollte gesondert erklärt werden. Den Beschäftigten ist vor der Einwilligung Gelegenheit zu geben, die Betriebsvereinbarung zur Kenntnis zu nehmen.

4. Zum weiteren Inhalt einer Betriebsvereinbarung: Es ist zu empfehlen, sämtliche Fragen zur Privatnutzung in der Betriebsvereinbarung zu regeln. In der Betriebsvereinbarung sollten daher die Nutzungsregelungen (zeitlicher Umfang, Verhaltensregeln) und die Zugriffsmöglichkeiten (Einwilligung, insbesondere zu Art und Umfang von Kontrollen) eindeutig festgehalten sein.

5. Auf der Grundlage der Einwilligung darf eine Protokollierung der Internetnutzung sowie eine Auswertung der Protokolldaten entsprechend B.I. stattfinden. Eine personenbezogene Auswertung von Protokolldaten darf jedoch nur bei einem konkreten Verdacht erfolgen. In Betracht

[4] Siehe A II 1.

kommt insbesondere der Verdacht eines Verstoßes gegen in der Betriebsvereinbarung festgeschriebene Verhaltensvorschriften bzw. den festgelegten Umfang der erlaubten Privatnutzung. Eine personenbezogene Kontrolle ist nur zulässig, wenn sie verhältnismäßig ist.

6. Beschäftigte, die diese Bedingungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden arbeitsrechtlichen Nachteil verweigern. Eine Privatnutzung ist dann nicht erlaubt. Da für diese Beschäftigten im Ergebnis nur die betriebliche Nutzung erlaubt ist, gelten für sie die Ausführungen unter B.I.

II. Nutzung des betrieblichen E-Mail-Accounts

1. Ist die private E-Mail-Nutzung erlaubt (oder gilt sie als erlaubt, s.o. [5]), ist der Arbeitgeber gegenüber den Beschäftigten und ihren Kommunikationspartnern zur Einhaltung des Fernmeldegeheimnisses verpflichtet.

Der Schutz des Fernmeldegeheimnisses gilt, solange der Übermittlungsvorgang andauert und die E-Mail noch nicht in den ausschließlichen Herrschaftsbereich des Empfängers gelangt ist. Dies ist beispielsweise der Fall, wenn sie sich noch in einem E-Mail-Postfach auf dem Server im Zugriffsbereich des Arbeitgebers befindet. Der Abschluss des Übermittlungsvorgangs hängt von den technischen Gegebenheiten, insbesondere dem verwendeten Übertragungsprotokoll, ab. Solange Nachrichten - wie bei Verwendung des „IMAP-Protokolls“ - auf einem zentralen E-Mail-Server des Arbeitgebers oder eines Providers verbleiben und bei jedem Zugriff durch die Beschäftigten erneut heruntergeladen werden, ist der Übermittlungsvorgang nicht beendet. Dies hat zur Folge, dass der Arbeitgeber grundsätzlich ohne Einwilligung der jeweiligen Beschäftigten nicht auf deren betriebliches E-Mail-Postfach zugreifen darf.

Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber grundsätzlich nur mit Einwilligung der betreffenden Beschäftigten erlaubt. Allerdings gelten gemäß §§ 88 Abs. 3, 91 ff. TKG die dort geregelten Ausnahmen (z.B. erforderliche Maßnahmen zum Schutz der technischen Systeme, d.h. zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen).

2. Der Arbeitgeber kann die Erlaubnis zur privaten Nutzung des betrieblichen E-Mail-Postfachs an Bedingungen knüpfen: In Betracht kommen Nutzungsregelungen (insbesondere zum zeitlichen Umfang; ggf. auch Verhaltensregeln) und Zugriffsmöglichkeiten des Arbeitgebers. Hierfür ist wiederum eine Einwilligung der Beschäftigten einzuholen. Wie schon bei der privaten Internetnutzung geht es hierbei zum einen um die Möglichkeit von Kontrollen (bezogen auf die o.g. Nut-

[5] Siehe A II 1.

zungsregelungen). Die Einwilligung sollte sich daher auf Art und Umfang solcher etwaiger Kontrollen beziehen.

Im Gegensatz zur privaten Internetnutzung steht jedoch bzgl. des privaten Mailverkehrs eine andere Zugriffsmöglichkeit im Vordergrund: Im gemeinsamen betrieblichen Interesse sollte eindeutig im Vorfeld festgelegt werden, ob bzw. wie der Arbeitgeber auf die betrieblichen Mails im gemischt-privat-betrieblichen Postfach zugreifen kann.

Die Ausführungen unter C. I. 2-6 gelten hierfür entsprechend.

3. Der Arbeitgeber sollte also klare Vorgaben machen, welche Einstellungen die Beschäftigten vorzunehmen haben, wenn sie - geplant oder nicht geplant - abwesend sind (z.B. Abwesenheitsnotiz).

4. Wurden diese Einstellungen nicht vorgenommen (etwa weil es bei einer ungeplanten Abwesenheit nicht möglich war oder weil es vergessen wurde), darf ein Zugriff auf das betriebliche E-Mail-Postfach der betroffenen Beschäftigten, soweit dies für betriebliche Zwecke erforderlich ist, nur mit deren vorab eingeholter Einwilligung erfolgen.

5. Ein Zugriff auf bereits vor der Abwesenheit der jeweiligen Beschäftigten eingegangenen E-Mails ist ebenfalls nur zulässig, soweit dieser für betriebliche Zwecke erforderlich ist und vorab Einwilligungen der Beschäftigten eingeholt wurden.

6. Haben Beschäftigte im Zusammenhang mit der betrieblichen E-Mail-Nutzung in die Regelungen zur privaten Mailnutzung eingewilligt, sind sie darauf hinzuweisen, dass im Zusammenhang mit einer Archivierung (z.B. gem. § 257 HGB, § 147 AO) auch eine Archivierung ihrer privaten E-Mails erfolgen kann. Den Beschäftigten sollte jedoch Gelegenheit gegeben werden, private Mails zu löschen oder an ihren privaten Account weiterzuleiten.

D. Regelungen für Geheimnisträger

„Geheimnisträger“ i.d.S. sind Beschäftigte, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden (Betriebsrat, Jugend- und Ausbildungsvertretung, betrieblicher Datenschutzbeauftragter, Betriebsarzt, Gleichstellungsbeauftragte u.a.) und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen.

I. Internet

Grundsätzlich besteht keine Kontrollbefugnis des Arbeitgebers bzgl. der Internetnutzung der o.g. „Geheimnisträger“, z.B. der Betriebsräte.

II. Nutzung des betrieblichen E-Mail-Accounts

Bei den „Geheimnisträgern“ muss eine Kenntnisnahme des Arbeitgebers von den Verkehrs- und Inhaltsdaten ausgeschlossen werden. Es empfiehlt sich, für diese Stellen nicht personalisierte funktionsbezogene Postfächer (z.B. Betriebsrat@Unternehmen.de) einzurichten und diese von Kontrollen bzw. Auswertungen auszunehmen.

Neben den Belangen der „Geheimnisträger“ selbst, sind in gleichem Maße die schutzwürdigen Belange der einzelnen Beschäftigten, die mit dem jeweiligen „Geheimnisträger“ kommunizieren, zu beachten. Auch insofern sind Vorkehrungen zu treffen. Es ist daher dafür zu sorgen, dass E-Mails der Beschäftigten von bzw. an den jeweiligen „Geheimnisträger“ (ggf. aufgrund einer einschlägigen Betreffzeile) von dem Arbeitgeber nicht zur Kenntnis genommen werden. Den Beschäftigten sollte daher empfohlen werden, derartige Kommunikation über andere Wege (z.B. private E-Mail-Adresse, schriftlich oder telefonisch) zu führen. So kann eine Kenntnisnahme der Verkehrs- und Inhaltsdaten durch den Arbeitgeber vollkommen ausgeschlossen werden.

E. Empfehlungen der Aufsichtsbehörden

1. Es wird empfohlen, über die betriebliche und/oder private Nutzung des Internets und des betrieblichen E-Mail-Accounts eine schriftliche Regelung zu treffen, in der die Fragen des Zugriffs, der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig festgelegt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

2. Sofern der Arbeitgeber seinen Beschäftigten die Möglichkeit zur Nutzung des betrieblichen E-Mail-Accounts für private E-Mail-Kommunikation ermöglichen möchte, sollte er bedenken, dass er dann an das Fernmeldegeheimnis gebunden ist. Dies führt in der Praxis regelmäßig zu erheblichen Konflikten, nämlich dann, wenn der Arbeitgeber für den Geschäftsablauf auf das betriebliche Postfach der Beschäftigten zugreifen möchte. Es wird daher empfohlen, dass der Arbeitgeber den Beschäftigten lediglich die private Nutzung des Internets anbietet, welche auch die Nutzung von Webmail-Diensten (wie z.B. web.de; gmx.de; yahoo.de etc.) umfasst. Anstatt der Nutzung der betrieblichen E-Mail-Accounts sollten die Beschäftigten dann auf die ausschließliche Nutzung privater Web-Mail-Accounts für private Nachrichten verwiesen werden. Das jeweilige betriebliche Postfach wird dann weiterhin ausschließlich betrieblich genutzt (vgl. B II).

3. Wenn der Arbeitgeber seinen Beschäftigten die private Nutzung des betrieblichen E-Mail-Accounts erlaubt hat (vgl. C II) und für den Geschäftsablauf auf das betriebliche Mailpostfach der einzelnen Beschäftigten zugreifen möchte, hat er Folgendes zu beachten: E-Mails mit erkennbar privatem Inhalt dürfen von dem Arbeitgeber nur in dem Umfang zur Kenntnis genommen werden, wie dies von der Einwilligung gedeckt und unerlässlich ist, um sie von den betrieblichen E-Mails zu trennen. Dasselbe gilt für solche E-Mails, die der Kommunikation der Beschäftigten mit „Geheimnisträgern“ (Betriebsrat, Jugend- und Ausbildungsvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragte u.a.) dienen. Dies ist durch eine entsprechende Verfahrensgestaltung zu gewährleisten. Wenn sich im Rahmen der Sichtung aus dem Absender und/oder Betreff einer E-Mail Anhaltspunkte dafür ergeben, dass es sich um eine geschützte und dem Privatbereich zuzurechnende E-Mail handelt, ist der Vertreter des Arbeitgebers oder die von dem Arbeitgeber bestimmte Person nicht berechtigt, den Inhalt der E-Mail zur Kenntnis zu nehmen, zu verarbeiten oder zu nutzen.

4. Wenn Beschäftigte das Unternehmen verlassen, sollte darauf geachtet werden, dass die persönliche betriebliche E-Mail-Adresse schnellstmöglich deaktiviert wird.

5. Ergänzende Hinweise lassen sich den Orientierungshilfen „Protokollierung“ und „zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ entnehmen.

F. Spamfilter und Virenschutz

Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie Inhalte aufweisen, die zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen können (Virenfilterung). Davon zu unterscheiden ist die Ausfilterung bzw. Veränderung von „Spam-Mails“. Beim Verfahren zur Behandlung von Spam-Mails ist § 303 a StGB zu beachten.

1. **Spamfilter**

   Über eine zentrale Spam-Filterung ist im Vorfeld zu unterrichten. Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Aus den in Betracht kommenden Varianten sollte die datenschutzfreundlichste gewählt werden. Zugleich sollte folgenden Grundsätzen Rechnung getragen werden:

   - Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.

- Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
- Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie selbst über den Umgang mit den an sie gerichteten E-Mails entscheiden können.

2. Virenschutz

Das Herausfiltern und Untersuchen von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist hinsichtlich privater E-Mails nur in dem in § 100 TKG festgelegten Umfang gestattet.

Anhang 1:

Muster einer Betriebsvereinbarung für die private Nutzung des Internets

Hinweise:

- **Entsprechend der Darstellung unter C.I. wird im folgenden Muster zunächst davon ausgegangen, dass den Beschäftigten die private Internetnutzung (welche auch die Nutzung von Webmail-Diensten, wie z.B. web.de, gmx.net, umfasst) gestattet wird, eine private Nutzung des betrieblichen E-Mail Accounts jedoch verboten ist.**
- **Die Musterbetriebsvereinbarung behandelt ausschließlich datenschutzrechtliche Aspekte; ggf. sind darüber hinaus arbeitsrechtliche Fragestellungen zu beachten.**

Dieses Muster kann auch für den Erlass einer Richtlinie / Anweisung oder als Orientierung für im Arbeitsvertrag zu regelnde Punkte herangezogen werden, wenn im Unternehmen kein Betriebsrat existiert. Ebenso kann die Orientierungshilfe analog im öffentlichen Bereich angewandt werden; hierbei sind landesspezifische Vorschriften zu beachten.

Betriebsvereinbarung[6]

Zwischen

der A-GmbH

und

dem Betriebsrat der A-GmbH,

wird folgende Betriebsvereinbarung über die

"Nutzung von Internet und E-Mail"

geschlossen.

(Präambel)

1. Gegenstand und Geltungsbereich

1.1 Die Betriebsvereinbarung regelt die Grundsätze für die Nutzung der betrieblichen Kommunikationssysteme E-Mail und Internet.

1.2 Diese Betriebsvereinbarung gilt räumlich für den Betrieb der A-GmbH in …

1.3 Die Betriebsvereinbarung gilt persönlich für Beschäftigte der A-GmbH.

[6] Die Musterbetriebsvereinbarung stellt eine Empfehlung der Datenschutzaufsichtsbehörden dar. Sie ist den konkreten Gegebenheiten im Unternehmen anzupassen. Abweichungen sind möglich.

2. Betriebliche und/oder private Nutzung

Die Nutzung der von der Arbeitgeberin zur Verfügung gestellten Kommunikationssysteme und Endgeräte zur Nutzung von Internet ist grundsätzlich nur zu betrieblichen Zwecken gestattet. Das betriebliche E-Mail Postfach darf ausschließlich zur betrieblichen Kommunikation genutzt werden.

2.1 Die Gestattung der privaten Nutzung des Internetzugangs nach den Vorgaben dieser Betriebsvereinbarung erfolgt ausschließlich gegenüber denjenigen Beschäftigten, die zuvor gegenüber der Arbeitgeberin eine Einwilligung gemäß **Anlage 1** abgegeben haben.

2.2 Liegt eine Einwilligung vor, ist die private Nutzung des betrieblichen Internetzugangs im Umfang von [*Definition durch Vertragspartner*] zulässig.

2.3 Die Beschäftigten sind frei in ihrer Entscheidung, ob sie eine solche Einwilligung abgeben wollen. Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerruflich. Soweit die Einwilligung nicht erteilt wird oder widerrufen wurde, so ist nur eine betriebliche Nutzung zulässig.

3. Verhaltensgrundsätze

3.1 Unzulässig ist jede vorsätzliche Nutzung der betrieblichen Kommunikationssysteme, die den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit schadet oder die gegen geltende Rechtsvorschriften verstößt. Dazu zählen

- der Abruf von für den Arbeitgeber kostenpflichtigen Internetseiten,
- das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver) oder
- Aktivitäten, die sich gegen das Unternehmen richten (sog. Compliance-Verstöße [*von Vertragspartnern zu konkretisieren*])
- …

3.2 [*Hinweise, soweit bestimmte Internetseiten/ - dienste gesperrt werden (black-lists)*]

3.3 Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen ist der Download von Programmen aus dem Internet nicht gestattet.

4. Nutzungsregelungen und Zugriffsrechte

4.1 [*ggf. allgemeine Regelungen zum Herunterladen von Inhalten, Speicherungen von Anhängen/Dateien, Möglichkeit bzw. Pflicht zur Verschlüsselung von E-Mails etc.*]

4.2 Bei geplanter Abwesenheit eines Beschäftigten ist durch den Beschäftigten ein automatisierter Hinweis auf die Abwesenheit des Beschäftigten sowie auf seine Vertretung einzurichten. Soweit

dies für betriebliche Zwecke erforderlich ist, kann ein Vertretungsassistent eingerichtet werden bzw. können eingehende E-Mails automatisiert an einen Vertreter weitergeleitet werden.

4.3 a) Wurde eine Abwesenheitsnachricht entgegen 4.2 nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.

b) Eine automatisierte Weiterleitung wird nur in dringend erforderlichen Fällen eingerichtet, insbesondere soweit eine Abwesenheitsnachricht allein den betrieblichen Erfordernissen nicht gerecht wird.

c) Ein Zugriff auf das betriebliche E-Mail-Postfach des betroffenen Beschäftigten für betriebliche Zwecke - etwa wenn Inhalte des Postfachs für die weitere Bearbeitung benötigt werden - darf darüber hinaus nur erfolgen, soweit dies für betriebliche Zwecke erforderlich ist.

Derartige Zugriffe können unter Hinzuziehung von Vertrauenspersonen [*konkret zu benennen*] im Vier-Augen-Prinzip durchgeführt werden. Der Beschäftigte wird über den Zugriff unverzüglich unterrichtet. Erkennbar private E-Mails und solche, die der Kommunikation des Beschäftigten mit den unter 4.6 angesprochenen Stellen dienen, dürfen inhaltlich nicht zur Kenntnis genommen werden.

4.4 Die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail Postfachs werden zur Sicherstellung der Funktionsfähigkeit des Systems im Abstand von … Tagen gespeichert und für maximal ... Jahre aufbewahrt.

4.5 Um gesetzlich vorgegebenen Aufbewahrungspflichten (z.B. gem. § 257 HGB, § 147 AO) gerecht zu werden, werden die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail Postfachs im Abstand von … Tagen archiviert und für maximal ... Jahre aufbewahrt.

4.6 Persönliche, aber geschäftlich veranlasste E-Mails (z.B. Kommunikation mit dem Betriebsrat, Betriebsarzt, Sozialberatung, Datenschutz oder Compliance Office) sollten über alternative Kommunikationswege abgewickelt werden (z.B. telefonisch, postalisch, private E-Mail-Adresse). Sollte dennoch derlei Kommunikation über das betriebliche E-Mail-Postfach abgewickelt werden, ist diese zu löschen bzw. lokal abzuspeichern. Bei einem Zugriff erkannte derartige Kommunikation (z.B. anhand des Betreffs bzw. Kommunikationspartners) darf inhaltlich nur durch den vorgesehenen Empfänger zur Kenntnis genommen werden.

5. Funktionspostfächer

E-Mail-Postfächer und die Internetkommunikation von Personen, die einer besonderen Vertraulichkeit unterliegen, sind von den Kontrollen nach dieser Vereinbarung ausgeschlossen. Eine Aufstellung dieser Postfächer findet sich in **Anlage 2**.

6. Spamfilter und Virenschutz

6. 1 Durch eine zentrale Spamfilterung können Spammails erkannt werden, indem auf eingehenden E-Mails zugegriffen wird. Erkannte Spammails werden im Betreff mit dem Wort „Spam“ markiert

und an den Empfänger weitergeleitet. Dieser hat sorgfältig zu prüfen, inwieweit es sich tatsächlich um eine Spam-Nachricht handelt. Ist dies zutreffend sollte diese unverzüglich gelöscht werden und der Erhalt derartiger E-Mails möglichst unterbunden werden.

6.2 Liegen konkrete Anhaltspunkte dafür vor, dass eine E-Mail Schadsoftware enthält, so wird diese automatisiert herausgefiltert und untersucht. Bestätigt sich der Verdacht, findet eine Weiterleitung an den Empfänger nur statt, wenn zuvor die entsprechenden Teilinhalte oder Anlagen entfernt wurden und Störungen oder Schäden durch die Weiterleitung ausgeschlossen werden können.

7. Verhaltenskontrolle

Die bei der Nutzung des betrieblichen E-Mail-Postfachs und des Internets anfallenden personenbezogenen Daten werden nur im Rahmen dieser Betriebsvereinbarung kontrolliert; insofern findet eine Verhaltenskontrolle statt. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften. Darüber hinausgehende Leistungs- und Verhaltenskontrollen werden nicht durchgeführt.

8. Protokollierung

8.1 Die Nutzung des Internets wird, soweit dies für die Gewährleistung der Systemsicherheit und/oder der Funktionsfähigkeit der eingesetzten IT-Systeme erforderlich ist, mit folgenden Informationen für jedes aufgerufene Objekt protokolliert:

- Datum/Uhrzeit
- Benutzerkennung
- IP-Adresse
- Zieladresse
- übertragene Datenmenge
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.2 Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:

- Datum/Uhrzeit
- Absender- und Empfängeradresse
- Message ID
- Nachrichtengröße
- Betreff
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.3 Die Protokolldaten nach Ziffer 8.1 und 8.2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit,
- Aktualisierung der Liste gesperrter Internet-Seiten („Black List“)
- Optimierung des Netzes und
- Datenschutzkontrolle

verwendet.

8.4 Die Protokolldaten nach Ziffer 8.1 werden für maximal …[7] Tage, Protokolldaten nach Ziffer 8.2 werden für maximal … Tage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert. Die Regelungen zur Zweckbindung aus § 31 des Bundesdatenschutzgesetzes sind zu beachten.

8.5 Personal, das Zugang zu Protokollinformationen hat, wird besonders auf die Sensibilität dieser Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet. Bei der Auswahl des Personals ist dies als Eignungsvoraussetzung zu berücksichtigen. Dafür wird auch (z.B. durch vertragliche Vereinbarung) Sorge getragen, wenn und soweit es sich nicht um eigenes Personal handelt.

9. Kontrollen

9.1 Zur Aktualisierung der gesperrten Internetseiten (Black-List) und zur Analyse von

- deutlich über dem üblichen Nutzungsverhalten liegende, auffällige Häufungen im Kommunikationsverhalten oder
- extensivem Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externen E-Mail-Domänen

kann die geschäftliche und private Nutzung von Internet und E-Mail mit folgenden Kontrolldaten für einen Zeitraum von einem Monat protokolliert und getrennt von den Protokolldaten nach Ziffer 8.1 und Ziffer 8.2. gespeichert werden:

- Gruppenzugehörigkeit,[8]
- Datum und Uhrzeit,
- genutzte externen E-Mail-Domänen,
- aufgerufene Internetdomänen (URLs),
- übertragene Datenmengen.

Für die Analysen werden statistische Aufbereitungen der protokollierten Kontrolldaten angefertigt, indem die im Zeitraum der Protokollierung auffällig häufig aufgerufenen Domänen und Übertragungsvolumina für Internet und E-Mail dargestellt sind (Domänanalysen). Diese Kontrolldaten werden durch den Arbeitgeber monatlich oder aus gegebenem Anlass gesichtet und ausgewertet.

9.2 Ergeben sich bei der Auswertung der Daten nach Ziffer 9.1. Hinweise auf unzulässige Zugriffe gem. Ziffer 3.1 oder auf eine Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Gleichzeitig wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) nach einem gesondert festzulegenden Verfahren stattfinden kann. An

[7] Die Speicherdauer ist je nach den Umständen des Einzelfalls auf das erforderliche Maß zu begrenzen. In der Praxis der Aufsichtsbehörden hat sich dabei eine Frist von wenigen Tagen als in der Regel ausreichend herausgestellt. Der Grundsatz der Datensparsamkeit ist zu beachten. Von den Möglichkeiten zur Anonymisierung und/oder Pseudonymisierung ist zum frühestmöglichen Zeitpunkt Gebrauch zu machen. Protokolldateien zu Zwecken der Gewährleistung der Datensicherheit sind regelmäßig auszuwerten.

[8] Zur Eingrenzung des Personenkreises bei missbräuchlicher Nutzung können gruppenbezogen Nutzungsdaten erhoben werden. Eine Gruppe sollte mindestens so viele Mitarbeiter enthalten, dass keine Identifizierung droht.

der Festlegung des Verfahrens der Auswertung von Protokolldaten sind der Betriebsrat, die IT-Abteilung und der betriebliche Datenschutzbeauftragte zu beteiligen. Das Verfahren ist den Beschäftigten bekannt zu geben.

9.3 Für die gezielte Kontrolle (personenbezogene Auswertung) entsprechend Stufe 3 müssen der genaue Zweck, der Umfang der Daten, der Zeitraum der Auswertung vorab in einem Konzept festgelegt und angekündigt werden; der Umfang der von der Auswertung erfassten Personen muss dabei auf den Kreis der nach § 32 Abs. 1 Satz 2 BDSG Betroffenen begrenzt werden. Es dürfen nicht sämtliche Beschäftigte überwacht werden. Die personenbezogenen Daten sind nach Beendigung des Verfahrens zu löschen. Über das Ergebnis der Auswertung wird der Beschäftigte schriftlich in Kenntnis gesetzt. Ihm ist Gelegenheit zur Stellungnahme zu geben. Entsprechend der Ergebnisse der Auswertung ist das weitere Vorgehen (Stufe 4) abzuwägen:

- Einstellen der Kontrollen/keine weitere Überwachung,
- erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Kontrolle oder
- Verschärfen der Kontrolle, in dem die Protokollierung auf dem Arbeitsplatzrechner stattfindet.

Die Durchführung weiterer arbeitsrechtlicher Maßnahmen bleibt hiervon unberührt.

9.4 Für die Protokollierung auf dem Arbeitsplatzrechner (Stufe 4) gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Beschäftigten müssen über diese Maßnahme nachträglich aufgeklärt werden.

9.5 Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts bei der Internet- oder E-Mail-Nutzung, Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 über einen Zeitraum bis zu maximal … Tagen aufzubewahren und personenbezogen auszuwerten.

Erweist sich der Verdacht als unbegründet oder werden die Protokolldateien nicht mehr zu weitergehenden Maßnahmen nach Ziffer 8 dieser Vereinbarung benötigt, so hat die Stelle, die eine Speicherung der Protokolldaten über … Tage hinaus veranlasst hat, unverzüglich die Löschung dieser Daten durch die IT-Abteilung zu veranlassen. Die erfolgte Löschung ist schriftlich gegenüber der beauftragenden Stelle durch die IT-Abteilung zu bestätigen. Die Betroffenen werden nach Abschluss der Maßnahmen unverzüglich darüber benachrichtigt.

9.6 Ein Verstoß gegen diese Betriebsvereinbarung kann arbeitsrechtliche Konsequenzen haben.

Darüber hinaus kann ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen, z.B. bei Nutzung kostenpflichtiger Internetseiten.

Die Arbeitgeberin behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs und des betrieblichen E-Mail Postfachs im Einzelfall zu untersagen.

10. Schulung der Beschäftigten

Die Beschäftigten werden in regelmäßig stattfindenden Schulungen mit den technischen Möglichkeiten und einer datenschutzgerechten Anwendung der eingesetzten Verfahren vertraut gemacht. Gleichzeitig werden sie über Art und Umfang der Erhebung und Verwendung ihrer personenbezogenen Daten informiert.

11. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten rechtzeitig mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden. Zur Evaluierung dieser Betriebsvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.

12. Schlussbestimmungen

12.1 Die Unwirksamkeit einzelner Bestimmungen dieser Vereinbarung führt nicht zur Unwirksamkeit der übrigen Regelungen. Im Falle der Unwirksamkeit einzelner Regelungen werden Betriebsrat und Arbeitgeberin unverzüglich Verhandlungen über eine Neuregelung des jeweiligen Sachverhalts aufnehmen.

12.2 Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist … gekündigt werden.

12.3 Im Falle einer Kündigung dieser Betriebsvereinbarung gelten diese Regelungen bis zum Abschluss einer neuen Vereinbarung. Nach Eingang der Kündigung verpflichten sich die Betriebsparteien, unverzüglich Verhandlungen über eine neue Betriebsvereinbarung aufzunehmen.

Anlagen:

- Anlage 1:
  Einwilligungserklärung zur privaten Nutzung des betrieblichen Internets
- Anlage 2:
  Von den Kontrollen ausgenommene E-Mail-Postfächer

Ort, den xx.xx.xxxx	Ort, den xx.xx.xxxx
_____	_____
A-GmbH	Betriebsrat der A-GmbH

Anlage 1 zur Musterbetriebsvereinbarung (Anhang 1): Einwilligungserklärung

Einwilligungserklärung zur privaten Nutzung des betrieblichen Internetzugangs

Ich möchte von dem Angebot Gebrauch machen, den betrieblichen Internetzugang in geringfügigem Umfang [*konkret bestimmen*] auch für private Zwecke zu nutzen.

1. Ich habe die Gelegenheit gehabt, die Betriebsvereinbarung über die Nutzung von Internet und E-Mail zur Kenntnis zu nehmen und bin mir über die folgenden, mit der Privatnutzung des Internets verbundenen Nutzungsbedingungen bewusst:

- Die private Nutzung ist nur in geringfügigem Umfang [*konkret bestimmen*]gestattet und nur sofern und soweit dadurch die geschäftliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für geschäftliche Zwecke nicht beeinträchtigt werden.
- Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet, sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.
- Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere
  - der Abruf für den Arbeitgeber kostenpflichtigen Internetseiten,
  - das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
  - Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver) oder
  - Aktivitäten, die sich gegen das Unternehmen richten (z.B. Compliance-Verstöße [*konkret benennen*])
  - […*an Regelung in Betriebsvereinbarung anpassen*]

  ist unzulässig.
- Die A-GmbH ist berechtigt, den Aufruf bestimmter Internet-Seiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internet-Inhalte.

2. Ich willige ein, dass auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe im Rahmen der Betriebsvereinbarung vom [*Datum einsetzen*] verarbeitet und unter den Voraussetzungen der Ziffern 8. und 9. der Betriebsvereinbarung protokolliert sowie personenbezogen ausgewertet werden.

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gem. § 88 TKG verzichte.

Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs das Internet nicht mehr privat nutzen darf.

Ort, Datum Unterschrift des Beschäftigten

_____ _____

Anlage 2 zur Musterbetriebsvereinbarung (Anhang 1): Ausgenommene E-Mail-Postfächer

Von den Kontrollen ausgenommene E-Mail-Postfächer

Aufgrund gesetzlicher Verschwiegenheitsverpflichtungen von den Kontrollen ausgenommene E-Mail-Postfächer / Funktionspostfächer:

- Betriebsarzt:
- Betriebsrat:
- Datenschutzbeauftragter:
- usw.

Anhang 2:
Muster einer Betriebsvereinbarung für die private Nutzung des Internets und des betrieblichen E-Mail-Postfachs

Hinweise:

- **Entsprechend der Darstellung unter C.II. wird im folgenden Muster davon ausgegangen, dass den Beschäftigten die private Nutzung des Internets und des betrieblichen E-Mail Postfachs gestattet wird. Die Musterbetriebsvereinbarung behandelt ausschließlich datenschutzrechtliche Aspekte; ggf. sind darüber hinaus arbeitsrechtliche Fragestellungen zu beachten.**
- **Die Musterbetriebsvereinbarung behandelt ausschließlich datenschutzrechtliche Aspekte; ggf. sind darüber hinaus arbeitsrechtliche Fragestellungen zu beachten.**

Dieses Muster kann auch für den Erlass einer Richtlinie / Anweisung oder als Orientierung für im Arbeitsvertrag zu regelnde Punkte herangezogen werden, wenn im Unternehmen kein Betriebsrat existiert. Ebenso kann die Orientierungshilfe analog im öffentlichen Bereich angewandt werden; hierbei sind landesspezifische Vorschriften zu beachten.

Betriebsvereinbarung[9]

Zwischen

der A-GmbH

und

dem Betriebsrat der A-GmbH,

wird folgende Betriebsvereinbarung über die

"Nutzung von Internet und E-Mail"

geschlossen.

(Präambel)

1. Gegenstand und Geltungsbereich

1.1 Die Betriebsvereinbarung regelt die Grundsätze für die Nutzung der betrieblichen Kommunikationssysteme E-Mail und Internet.

1.2 Diese Betriebsvereinbarung gilt räumlich für den Betrieb der A-GmbH in …

1.3 Die Betriebsvereinbarung gilt persönlich für Beschäftigte der A-GmbH.

[9] Die Musterbetriebsvereinbarung stellt eine Empfehlung der Datenschutzaufsichtsbehörden dar. Sie ist den konkreten Gegebenheiten im Unternehmen anzupassen. Abweichungen sind möglich.

2. Betriebliche und/oder private Nutzung

Die Nutzung der von der Arbeitgeberin zur Verfügung gestellten Kommunikationssysteme und Endgeräte zur Nutzung von E-Mail und Internet ist grundsätzlich nur zu betrieblichen Zwecken gestattet.

2.1 Die Gestattung der privaten Nutzung des Internetzugangs und des betrieblichen E-Mail-Postfachs nach den Vorgaben dieser Betriebsvereinbarung erfolgt ausschließlich gegenüber denjenigen Beschäftigten, die zuvor gegenüber der Arbeitgeberin eine Einwilligung gemäß **Anlage 1** abgegeben haben.

2.2 Liegt eine Einwilligung vor, ist die private Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail Postfachs im Umfang von [*Definition durch Vertragspartner*] zulässig.

2.3 Die Beschäftigten sind frei in ihrer Entscheidung, ob sie eine solche Einwilligung abgeben wollen. Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerruflich. Soweit die Einwilligung nicht erteilt wird oder widerrufen wurde, so ist nur eine betriebliche Nutzung zulässig.

3. Verhaltensgrundsätze

3.1 Unzulässig ist jede vorsätzliche Nutzung der betrieblichen Kommunikationssysteme, die den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit schadet oder die gegen geltende Rechtsvorschriften verstößt. Dazu zählen

- der Abruf von für den Arbeitgeber kostenpflichtigen Internetseiten,
- das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver) oder
- Aktivitäten, die sich gegen das Unternehmen richten (sog. Compliance-Verstöße [*von Vertragspartnern zu konkretisieren*])
- …

3.2 [*Hinweise, soweit bestimmte Internetseiten/ - dienste gesperrt werden (black-lists)*]

3.3 Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen ist der Download von Programmen aus dem Internet nicht gestattet.

4. Nutzungsregelungen und Zugriffsrechte

4.1 [*ggf. allgemeine Regelungen zum Herunterladen von Inhalten, Speicherungen von Anhängen/Dateien, Möglichkeit bzw. Pflicht zur Verschlüsselung von E-Mails etc.]*
Gesendete und empfangene private E-Mails sind in einen Ordner „Privates“ zu verschieben bzw. zu löschen.

4.2 Bei geplanter Abwesenheit eines Beschäftigten ist durch den Beschäftigten ein automatisierter Hinweis auf die Abwesenheit des Beschäftigten sowie auf seine Vertretung einzurichten. Soweit dies für betriebliche Zwecke erforderlich ist, kann ein Vertretungsassistent eingerichtet werden bzw. können eingehende E-Mails automatisiert an einen Vertreter weitergeleitet werden.

4.3 a) Wurde eine Abwesenheitsnachricht entgegen 4.2 nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.

b) Eine automatisierte Weiterleitung wird nur in dringend erforderlichen Fällen eingerichtet, insbesondere soweit eine Abwesenheitsnachricht allein den betrieblichen Erfordernissen nicht gerecht wird.

c) Ein Zugriff auf das betriebliche E-Mail-Postfach des betroffenen Beschäftigten für betriebliche Zwecke - etwa wenn Inhalte des Postfachs für die weitere Bearbeitung benötigt werden – darf darüber hinaus nur erfolgen, soweit dies für betriebliche Zwecke erforderlich ist.

Derartige Zugriffe können unter Hinzuziehung von Vertrauenspersonen [konkret zu benennen] im Vier-Augen-Prinzip durchgeführt werden. Der Beschäftigte wird über den Zugriff unverzüglich unterrichtet. Erkennbar private E-Mails und solche, die der Kommunikation des Beschäftigten mit den unter 4.7 angesprochenen Stellen dienen, dürfen inhaltlich nicht zur Kenntnis genommen werden.

4.4 Vor seinem Ausscheiden hat der Beschäftigte seine privaten Mails bzw. den Ordner „Privates“ aus dem betrieblichen E-Mail Postfach zu entfernen. **Ihm ist dazu eine angemessene Zeit** [*konkret festzulegen*] **einzuräumen**.

4.5 Die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail Postfachs werden zur Sicherstellung der Funktionsfähigkeit des Systems im Abstand von … Tagen gespeichert und für maximal ... Jahre aufbewahrt. Davon können bei erlaubter Privatnutzung des betrieblichen E-Mail-Postfachs auch private E-Mails betroffen sein, soweit sie nicht vor der Speicherung gelöscht bzw. in einen als „persönlich“ gekennzeichneten Ordner abgelegt wurden. Solche E-Mails werden nicht für den genannten Zweck gespeichert. Vor seinem Ausscheiden hat der Beschäftigte seinen persönlichen Ordner zu löschen. **Ihm ist dazu eine angemessene Zeit** [*konkret festzulegen*] **einzuräumen**.]

4.6 Um gesetzlich vorgegebenen Aufbewahrungspflichten (z.B. gem. § 257 HGB, § 147 AO) gerecht zu werden, werden die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail Postfachs im Abstand von … Tagen archiviert und für maximal ... Jahre aufbewahrt. Davon können bei erlaubter Privatnutzung des betrieblichen E-Mail-Postfachs auch private E-Mails betroffen sein, soweit sie nicht vor der Archivierung gelöscht bzw. in einen als „persönlich“ gekennzeichneten Ordner abgelegt wurden. Vor seinem Ausscheiden hat der Beschäftigte seinen persönlichen Ordner zu löschen. **Ihm ist dazu eine angemessene Zeit** [*konkret festzulegen*] **einzuräumen**.]

4.7 Persönliche, aber geschäftlich veranlasste E-Mails (z.B. Kommunikation mit dem Betriebsrat, Betriebsarzt, Sozialberatung, Datenschutz oder Compliance Office) sollten über alternative Kommunikationswege abgewickelt werden (z.B. telefonisch, postalisch, private E-Mail-Adresse). Sollte dennoch derlei Kommunikation über das betriebliche E-Mail-Postfach abgewickelt werden, ist diese zu löschen bzw. lokal abzuspeichern. Bei einem Zugriff erkannte derartige Kommunikation (z.B. anhand

des Betreffs bzw. Kommunikationspartners) darf inhaltlich nur durch den vorgesehenen Empfänger zur Kenntnis genommen werden.

5. Funktionspostfächer

E-Mail-Postfächer und die Internetkommunikation von Personen, die einer besonderen Vertraulichkeit unterliegen, sind von den Kontrollen nach dieser Vereinbarung ausgeschlossen. Eine Aufstellung dieser Postfächer findet sich in **Anlage 2**.

6. Spamfilter und Virenschutz

6.1 Durch eine zentrale Spamfilterung können Spammails erkannt werden, indem auf eingehenden E-Mails zugegriffen wird. Bei erlaubter Privatnutzung des betrieblichen E-Mail-Postfachs wird auch auf den Betreff und den Inhalt privater E-Mails zugegriffen. Erkannte Spammails werden im Betreff mit dem Wort „Spam“ markiert und an den Empfänger weitergeleitet. Dieser hat sorgfältig zu prüfen, inwieweit es sich tatsächlich um eine Spam-Nachricht handelt. Ist dies zutreffend sollte diese unverzüglich gelöscht werden und der Erhalt derartiger E-Mails möglichst unterbunden werden.

6.2 Liegen konkrete Anhaltspunkte dafür vor, dass eine E-Mail Schadsoftware enthält, so wird diese automatisiert herausgefiltert und untersucht. Bestätigt sich der Verdacht, findet eine Weiterleitung an den Empfänger nur statt, wenn zuvor die entsprechenden Teilinhalte oder Anlagen entfernt wurden und Störungen oder Schäden durch die Weiterleitung ausgeschlossen werden können.

7. Verhaltenskontrolle

Die bei der Nutzung des betrieblichen E-Mail-Postfachs und des Internets anfallenden personenbezogenen Daten werden nur im Rahmen dieser Betriebsvereinbarung kontrolliert; insofern findet eine Verhaltenskontrolle statt. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften. Darüber hinausgehende Leistungs- und Verhaltenskontrollen werden nicht durchgeführt.

8. Protokollierung

8.1 Die Nutzung des Internets wird, soweit dies für die Gewährleistung der Systemsicherheit und/oder der Funktionsfähigkeit der eingesetzten IT-Systeme erforderlich ist, mit folgenden Informationen für jedes aufgerufene Objekt protokolliert:

- Datum/Uhrzeit
- Benutzerkennung
- IP-Adresse
- Zieladresse
- übertragene Datenmenge
- ... *[abschließende Aufzählung aller Protokolldaten]*

8.2 Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:

- Datum/Uhrzeit
- Absender- und Empfängeradresse
- Message ID
- Nachrichtengröße
- Betreff
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.3 Die Protokolldaten nach Ziffer 8.1 und 8.2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit,
- Aktualisierung der Liste gesperrter Internet-Seiten („Black List“)
- Optimierung des Netzes und
- Datenschutzkontrolle

verwendet.

8.4 Die Protokolldaten nach Ziffer 8.1 werden für maximal …[10] Tage, Protokolldaten nach Ziffer 8.2 werden für maximal … Tage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert. Die Regelungen zur Zweckbindung aus § 31 des Bundesdatenschutzgesetzes sind zu beachten.

8.5 Personal, das Zugang zu Protokollinformationen hat, wird besonders auf die Sensibilität dieser Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet. Bei der Auswahl des Personals ist dies als Eignungsvoraussetzung zu berücksichtigen. Dafür wird auch (z.B. durch vertragliche Vereinbarung) Sorge getragen, wenn und soweit es sich nicht um eigenes Personal handelt.

9. Kontrollen

9.1 Zur Aktualisierung der gesperrten Internetseiten (Black-List) und zur Analyse von

- deutlich über dem üblichen Nutzungsverhalten liegende, auffällige Häufungen im Kommunikationsverhalten oder
- extensivem Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externen E-Mail-Domänen

kann die geschäftliche und private Nutzung von Internet und E-Mail mit folgenden Kontrolldaten für einen Zeitraum von einem Monat protokolliert und getrennt von den Protokolldaten nach Ziffer 8.1 und Ziffer 8.2. gespeichert werden:

[10] Die Speicherdauer ist je nach den Umständen des Einzelfalls auf das erforderliche Maß zu begrenzen. In der Praxis der Aufsichtsbehörden hat sich dabei eine Frist von wenigen Tagen als in der Regel ausreichend herausgestellt. Der Grundsatz der Datensparsamkeit ist zu beachten. Von den Möglichkeiten zur Anonymisierung und/oder Pseudonymisierung ist zum frühestmöglichen Zeitpunkt Gebrauch zu machen. Protokolldateien zu Zwecken der Gewährleistung der Datensicherheit sind regelmäßig auszuwerten.

- Gruppenzugehörigkeit,[11]
- Datum und Uhrzeit,
- genutzte externen E-Mail-Domänen,
- aufgerufene Internetdomänen (URLs),
- übertragene Datenmengen.

Für die Analysen werden statistische Aufbereitungen der protokollierten Kontrolldaten angefertigt, indem die im Zeitraum der Protokollierung auffällig häufig aufgerufenen Domänen und Übertragungsvolumina für Internet und E-Mail dargestellt sind (Domänanalysen). Diese Kontrolldaten werden durch den Arbeitgeber monatlich oder aus gegebenem Anlass gesichtet und ausgewertet.

Für die Analysen werden statistische Aufbereitungen der protokollierten Kontrolldaten angefertigt, indem die im Zeitraum der Protokollierung auffällig häufig aufgerufenen Domänen und Übertragungsvolumina für Internet und E-Mail dargestellt sind (Domänanalysen). Diese Kontrolldaten werden durch den Arbeitgeber monatlich oder aus gegebenem Anlass gesichtet und ausgewertet.

9.2 Ergeben sich bei der Auswertung der Daten nach Ziffer 9.1. Hinweise auf unzulässige Zugriffe gem. Ziffer 3.1 oder auf eine Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Gleichzeitig wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) nach einem gesondert festzulegenden Verfahren stattfinden kann. An der Festlegung des Verfahrens der Auswertung von Protokolldaten sind der Betriebsrat, die IT-Abteilung und der betriebliche Datenschutzbeauftragte zu beteiligen. Das Verfahren ist den Beschäftigten bekannt zu geben.

9.3. Für die gezielte Kontrolle (personenbezogene Auswertung) entsprechend Stufe 3 müssen der genaue Zweck, der Umfang der Daten, der Zeitraum der Auswertung vorab in einem Konzept festgelegt und angekündigt werden; der Umfang der von der Auswertung erfassten Personen muss dabei auf den Kreis der nach § 32 Abs. 1 Satz 2 BDSG Betroffenen begrenzt werden. Es dürfen nicht sämtliche Beschäftigte überwacht werden. Die personenbezogenen Daten sind nach Beendigung des Verfahrens zu löschen. Über das Ergebnis der Auswertung wird der Beschäftigte schriftlich in Kenntnis gesetzt. Ihm ist Gelegenheit zur Stellungnahme zu geben. Entsprechend der Ergebnisse der Auswertung ist das weitere Vorgehen (Stufe 4) abzuwägen:

- Einstellen der Kontrollen/keine weitere Überwachung,
- erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Kontrolle oder
- Verschärfen der Kontrolle, in dem die Protokollierung auf dem Arbeitsplatzrechner stattfindet.

Die Durchführung weiterer arbeitsrechtlicher Maßnahmen bleibt hiervon unberührt.

9.4. Für die Protokollierung auf dem Arbeitsplatzrechner (Stufe 4) gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Beschäftigten müssen über diese Maßnahme nachträglich aufgeklärt werden.

[11] Zur Eingrenzung des Personenkreises bei missbräuchlicher Nutzung können gruppenbezogen Nutzungsdaten erhoben werden. Eine Gruppe sollte mindestens so viele Mitarbeiter enthalten, dass keine Identifizierung droht.

9.5. Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts bei der Internet- oder E-Mail-Nutzung, Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 über einen Zeitraum bis zu maximal … Tagen aufzubewahren und personenbezogen auszuwerten.

Erweist sich der Verdacht als unbegründet oder werden die Protokolldateien nicht mehr zu weitergehenden Maßnahmen nach Ziffer **8** dieser Vereinbarung benötigt, so hat die Stelle, die eine Speicherung der Protokolldaten über … Tage hinaus veranlasst hat, unverzüglich die Löschung dieser Daten durch die IT-Abteilung zu veranlassen. Die erfolgte Löschung ist schriftlich gegenüber der beauftragenden Stelle durch die IT-Abteilung zu bestätigen. Die Betroffenen werden nach Abschluss der Maßnahmen unverzüglich darüber benachrichtigt.

9.6 Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts (u.a. Compliance-Verstoß) bei der Nutzung des betrieblichen E-Mail-Postfachs unter Beteiligung des Datenschutzbeauftragten im Vier-Augen-Prinzip Zugriff auf die gespeicherten E-Mails zu nehmen. [Anmerkungen: Ausführungen zu konkretem Verfahren: u.a. was unter einem Compliance-Verstoß zu verstehen ist, Verfahren selbst, beteiligte Personen, Dokumentation des Zugriffs und Informationen des betroffenen Beschäftigten]

9.7 Ein Verstoß gegen diese Betriebsvereinbarung kann arbeitsrechtliche Konsequenzen haben.

Darüber hinaus kann ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen, z.B. bei Nutzung kostenpflichtiger Internetseiten.

Die Arbeitgeberin behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs und des betrieblichen E-Mail Postfachs im Einzelfall zu untersagen.

10. Schulung der Beschäftigten

Die Beschäftigten werden in regelmäßig stattfindenden Schulungen mit den technischen Möglichkeiten und einer datenschutzgerechten Anwendung der eingesetzten Verfahren vertraut gemacht. Gleichzeitig werden sie über Art und Umfang der Erhebung und Verwendung ihrer personenbezogenen Daten informiert.

11. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten rechtzeitig mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden. Zur Evaluierung dieser Betriebsvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.

12. Schlussbestimmungen

12.1 Die Unwirksamkeit einzelner Bestimmungen dieser Vereinbarung führt nicht zur Unwirksamkeit der übrigen Regelungen. Im Falle der Unwirksamkeit einzelner Regelungen werden Betriebsrat und Arbeitgeberin unverzüglich Verhandlungen über eine Neuregelung des jeweiligen Sachverhalts aufnehmen.

12.2 Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist … gekündigt werden.

12.3 Im Falle einer Kündigung dieser Betriebsvereinbarung gelten diese Regelungen bis zum Abschluss einer neuen Vereinbarung. Nach Eingang der Kündigung verpflichten sich die Betriebsparteien, unverzüglich Verhandlungen über eine neue Betriebsvereinbarung aufzunehmen.

Anlagen:

- Anlage 1:
  Einwilligungserklärung zur privaten Nutzung des betrieblichen Internets und des betrieblichen E-Mail-Postfachs
- Anlage 2:
  Von den Kontrollen ausgenommene E-Mail-Postfächer

Ort, den xx.xx.xxxx	Ort, den xx.xx.xxxx
_____	_____
A-GmbH	Betriebsrat der A-GmbH

Anlage 1 zur Musterbetriebsvereinbarung (Anhang 2): Einwilligungserklärung

Einwilligungserklärung zur privaten Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail-Postfachs

Ich möchte von dem Angebot Gebrauch machen, den betrieblichen Internetzugang und das betriebliche E-Mail-Postfach in geringfügigem Umfang [*konkret bestimmen*] auch für private Zwecke zu nutzen.

1. Ich habe die Gelegenheit gehabt, die Betriebsvereinbarung über die Nutzung von Internet und E-Mail zur Kenntnis zu nehmen und bin mir über die folgenden, mit der Privatnutzung des Internets und des betrieblichen E-Mail Postfachs verbundenen Nutzungsbedingungen bewusst:

- Die private Nutzung ist nur in geringfügigem Umfang [*konkret bestimmen*]gestattet und nur sofern und soweit dadurch die geschäftliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für geschäftliche Zwecke nicht beeinträchtigt werden.
- Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet, sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.
- Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere
  - der Abruf für den Arbeitgeber kostenpflichtigen Internetseiten,
  - das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
  - Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver) oder
  - Aktivitäten, die sich gegen das Unternehmen richten (z.B. Compliance-Verstöße [*konkret benennen*])
  - […*an Regelung in Betriebsvereinbarung anpassen*]

  ist unzulässig.
- Die A-GmbH ist berechtigt, den Aufruf bestimmter Internet-Seiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internet-Inhalte.

2. Ich willige ein, dass

- **auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe und meine private E-Mail Kommunikation im Rahmen dieser Betriebsvereinbarung verarbeitet und unter den Voraussetzungen der Ziffern 8. und 9. der Betriebsvereinbarung protokolliert sowie personenbezogen ausgewertet werden,**
- **bei einer Abwesenheit meinerseits, entsprechend der Ziffer 4.3 der Betriebsvereinbarung ein Zugriff für betriebliche Zwecke auf mein betriebliches E-Mail-Postfach erfolgen darf und auch ein Hinweis auf meine Abwesenheit hinterlegt wird oder in dringend erforderlichen Fällen eine Weiterleitung auf das E-Mail Postfach meines Vertreters eingerichtet wird bzw. ein Zugriff des Arbeitgebers auf mein E-Mail Postfach ermöglicht wird,**

- **eine Speicherung meiner privaten E-Mails im Rahmen der Sicherstellung der IT-Sicherheit des Systems erfolgt, sofern ich diese nicht vor dem Zeitpunkt der Speicherung gelöscht bzw. in meinen Ordner „Privates“ verschoben habe,**
- **eine Archivierung meiner privaten E-Mails erfolgt, sofern ich diese nicht vor dem Zeitpunkt der Archivierung gelöscht bzw. in meinen Ordner „Privates“ verschoben habe.**

Im Rahmen einer gezielten Kontrolle nach Ziffer 9.2 wünsche ich die Einbeziehung folgender Vertrauenspersonen:

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gem. § 88 TKG verzichte. Mir ist weiter bekannt, dass bei der zentralen Spam-Filterung automatisch auf den Betreff oder Inhalte auch meiner privaten E-Mails zugegriffen wird. Mir ist auch bewusst, dass ich vor meinem Ausscheiden aus dem Unternehmen alle privaten E-Mails und meinen Ordner „Privates“ löschen muss.

Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs den Internetzugang und das betriebliche E-Mail Postfach nicht mehr privat nutzen darf.

Ort, Datum

_____

Unterschrift des Beschäftigten

_____

Anlage 2 zur Musterbetriebsvereinbarung (Anhang 2): Ausgenommene E-Mail-Postfächer

Von den Kontrollen ausgenommene E-Mail-Postfächer

Aufgrund gesetzlicher Verschwiegenheitsverpflichtungen von den Kontrollen ausgenommene E-Mail-Postfächer / Funktionspostfächer:

- Betriebsarzt:
- Betriebsrat:
- Datenschutzbeauftragter:
- usw.