Spreenauten GmbH
Meeraner Str. 11b
12681 Berlin. Germany

Fon
+49.(0)30.293.8197-0

Freecall Internationl
00800.11.88.44.00

Fax
+49.(0)30.293.8197-0

E-mail
support@spreenauten.com

Website
www.spreenauten.de

HRB
AG Berlin-Charlottenburg
136729B

UST-ID Deutschland
DE279088233

Richtlinie Informationssicherheit der Spreenauten GmbH

Executive Summary Informationssicherheit

Die Informationssicherheitsrichtlinie der Spreenauten GmbH beschreibt wie vertrauliche Informationen in der Spreenauten GmbH effektiv geschützt werden. Durch das sich stetig wandelnde IT Bedrohungsszenario stehen die wöchentlichen Schulungen & Updates unseres Team im Vordergrund. Der aktuelle Stand der Information Security Policy ist daher als Basis, nicht aber als vollumfängliche Beschreibung unserer Information Security zu verstehen.

Ziel

Das Ziel aller Maßnahmen unserer Informationssicherheit ist es unsere Informationen gegen den Zugriff von Dritten bzw. die Weitergabe bestmöglich und auf dem jeweils aktuellen Stand der Technik zu schützen.

Definition Informationen

Informationen ist sämtliches Wissen, das in unseren Geltungsbereich gelangt. Dabei ist es unerheblich auf welchem Wege dies geschieht. Gespräche (z.B. in Meetings) gehören hierzu ebenso wie Dateien jeglicher Art und das Wissen um Prozesse im Bezug auf unser Unternehmen und unsere Geschäftspartner.

Vertraulichkeit

Wir unterscheiden nicht zwischen vertraulichen und anderen Informationen, sondern gehen bei allen Informationen davon aus, dass diese ausschließlich mit individuellen Personen (und niemals mit Personengruppen) geteilt werden, die diese Informationen für Ihre Tätigkeit in unserem Unternehmen unbedingt benötigen und welche die entsprechende Sicherheitsfreigabe durch uns inne haben.

Verantwortlichkeiten

Informationssicherheit gehört zu den höchsten Prinzipien der Spreenauten GmbH. Das bedeutet, dass jeder Mitarbeiter für die Aufrechterhaltung der Informationssicherheit in seinem Bereich verantwortlich ist und Meldepflicht diesbezüglich hat.

Ansprechpartner Informationssicherheit

Informationssicherheits- & Datenschutzbeauftragte: Nico Ludvikova
privacy@spreenauten.com
CTO: Daniel Knappe dk@spreenauten.com
[Aktualisiert 15.03.2020]

Informationssicherheit durch schützende Prozesse

Prozesse

Prozesse beschreiben den Ablauf des Umgangs mit Informationen in unserem Unternehmen. Sie sind klare Handlungsanweisungen und definieren, im Bezug auf die Informationssicherheit der Spreenauten GmbH, welcher Mitarbeiter mit welchen Informationen arbeitet und wie mit diesem verfahren wird. Sie sind Gegenstand von fortlaufenden Anpassungen, z.B. an neue Risiko-Szenarien und werden in regelmäßigen Trainings von unseren Mitarbeitern verinnerlicht. Die Wirksamkeit und Anwendungen wird bei Audits sowie simulierten Angriffen getestet.

(Informations)Schützende Prozesse

Die Spreenauten GmbH schützt Informationen in Ihrem Einflussbereich durch die strikte Anwendung von präventiven und schützenden Prozessen, die weit über die zugrunde gelegten Richtlinien (-> 2.11) hinausgehen. Diese sind im Dokument “Schützende Prozesse der Spreenauten GmbH (C)” zu finden. Bei diesem Dokument handelt es sich um eine Ressource, die ausschließlich den betreffenden Mitarbeitern der Spreenauten GmbH zur Verfügung steht. Dritten werden sie nicht bekanntgegeben. In diesem Fall würde eine Veröffentlichung die von uns getroffenen Sicherheitsvorkehrungen zwar nicht schwächen, einem potentiellen Angreifer aber gestatten Überlegungen anzustellen, wie er diese umgehen kann.

Die folgenden Unterpunkte beziehen sich daher auf allgemeines best practice, welches natürlich auch bei uns Anwendung findet.

Social Engineering - Gegenmaßnahmen (Think First)

Die Spreenauten GmbH ist sich der Gefahr, welche Social Engineering betrifft, bewusst und erkennt diese als eines der wichtigsten Risikoszenarien für ihren Datenschutz. Also wichtigste Gegenmaßnahme sehen wir die Schulung und Aufrechterhaltung der Aufmerksamkeit unserer Mitarbeiter. Diese geschieht bei uns sowohl automatisiert über regelmäßige Surveys, welche fester Bestandteil unseres HR Systems sind, wie auch in den regelmäßigen Mitarbeitergesprächen. Die Wirksamkeit überprüfen wir durch regelmäßige simulierte Angriffe.

Siehe hierzu auch “IT Sicherheit Spreenauten GmbH (S. 16 Absatz 2 Angriffe / Social Hacking” (C).

Speicherung von Information

Weniger ist mehr. Die Spreenauten GmbH speichert nur solche Informationen, die für die Bearbeitung von Aufträgen sowie der Aufrechterhaltung von Geschäftsbeziehungen unbedingt notwendig sind. Darüber hinausgehende Informationen werden nicht gespeichert.

Die Speicherung von Informationen erfolgt verschlüsselt. Speicherort und Informationen werden durch effektive Zugriffskontrollen geschützt.

Siehe hierzu “Speicherung und Zugriffskontrolle auf Informationen der Spreenauten GmbH” (TS).

Teilen von Informationen

Informationen werden weiteren Mitarbeitern nur zugänglich gemacht, soweit diese sie für die Bearbeitung eines Auftrags benötigen. Einzige Ausnahme hierfür sind Informationen die unternehmensweite Projekte betreffen. Interne Informationssilos sind stets zu vermeiden.

So Informationen aus zwingenden Gründen weitergegeben werden müssen, geschieht dies ausschließlich an einzelne Mitarbeiter und nie an Gruppenverteiler. Basis hierfür ist das Dokument "Richtline zur internen Weitergabe von Informationen der Spreenauten GmbH" (C).

So Informationen aus zwingenden Gründen extern weitergegeben werden müssen, geschieht dies ausschließlich auf Basis der "Richtlinie zur externen Weitergabe von Informationen der Spreenauten GmbH" (C) . Ferner ist die Grundlage zur externen Weitergabe von Informationen, dass die Einhaltung Absatz 4 (Subsidiarität) dieses Dokuments sichergestellt ist.

Löschen von Informationen

Die Spreenauten GmbH bewahrt Informationen nur solange auf, so dies für die Bearbeitung eines Auftrags, der Aufrechterhaltung einer Geschäftsbeziehung oder aus rechtlichen Gründen notwendig ist.
Wenn keiner dieser Gründe auftritt werden Informationen gelöscht. Physische Informationsträger (z.B. Akten, DVDs) werden gemäß der DIN 66399 unter Einhaltung der Sicherheitsstufe 4 vernichtet.
Digitale Informationsträger (HD, SD etc.) werden gemäß des 5220-22-M Standards des US Verteidigungsministeriums gelöscht.

Einzelheiten regelt die Arbeitsanweisung "Datenschutzkonformes Löschen von Informationen" (C) der Spreenauten GmbH.

Zuständig für die Einhaltung dieses Punkts ist der aktuelle COO der Spreenauten GmbH.

Passwortsicherheit

Informationen, welche von der Spreenauten GmbH digital gespeichert werden, werden verschlüsselt und mit sicheren Passwörtern bzw. Keys geschützt.
Die von uns verwendeten Systeme erzwingen sichere Passwörter. Zugangsdaten werden in verschlüsselnden Apps (sog. Passwort Safes) gespeichert. Die Änderungen von Passwörtern wird in engen, jedoch bewusst unregelmäßigen, Intervallen systemseitig erzwungen.

Siehe hierzu auch "IT Sicherheit Spreenauten GmbH: Grundlagen - Schwerpunkt: Device" Seite 3 Absatz 2 "Passwortsicherheit".

Umgang mit informationsverarbeitender Technik

Die Spreenauten GmbH schult alle Mitarbeiter regelmäßig im sicheren und achtsamen Umgang mit informationsverabeitender Technik. Neben der oben erwähnten Passwortsicherheit liegt ein Fokus auf social Engineering (z.B. Phisihing) und der Gefahr von technischen Angriffen (z.B. Trojanern & Ramsoftware-Attacken). Der Schwerpunkt liegt auf dem richtigen Verhalten, dem Erkennen von Risiken, der richtigen Anwendung von defensiven Techniken sowie dem richtigen Reporting von

Sicherheitsproblemen bzw. Vorfällen.

Verantwortlich hierfür ist der:die aktuelle Informationssicherheits- & Datenschutzbeauftragte der Spreenauten GmbH. Näheres zum Umgang mit Informationsverarbeitender Technik ist im Dokument “IT Sicherheit Spreenauten GmbH: Grundlagen - Schwerpunkt: Devices” (C) zu finden.

Clean Desk Policy (CDP)

Die Spreenauten GmbH sieht die sogenannte “Clean Desk Policy” als einen der wirkungsvollsten Prozesse zum Schutz von Informationen.
Die Einhaltung dieser wird täglich kontrolliert. Dies gilt für Arbeitsplätze (Büro, Lager, Technik) ebenso wie für Konferenzräume & Firmenwagen.

Näheres regelt die “Clean Desk Policy der Spreenauten GmbH”,

Verantwortlich für die Umsetzung und Kontrolle ist der:die aktuelle Informationssicherheit- und Datenschutzbeauftragte.

Zugangsschutz

Die Räume der Spreenauten sind durch mehrere aufeinander abgestimmte Systeme und Prozesse zugangsgeschützt. Die Zugangsberechtigung sowie die Zugangsverweigerung erfolgt individuell. Akten- und Serverräume erzwingen eine mindestens 3-fache Identifizierung & Authentifizierung. Der physische Zugang erfolgt niemals durch einen Mitarbeiter alleine sondern immer in Begleitung. Die begleitende Person wird automatisiert und auf dem Zufallsprinzip beruhend bestimmt.

Zugrunde liegende Richtlinien

Die Spreenauten GmbH legt bei der Gestaltung und Umsetzung von schützenden Prozessen folgende Richtlinien zu Grunde:

ISO/IEC 27001
Information technology – Security techniques – Information security management systems – Requirements

BSI-Standard 200-1
Management Systems for Information Security

Interne Audits

Regelmäßige interne Audits, welche entweder automatisiert über unser HR System erzwungen werden bzw. in persönlichen Meetings stattfinden, stellen sicher, dass sich alle Mitarbeiter der Notwendigkeit von Prozessen, welche Informationen in unserem Geltungsbereich schützen betreffen, bewusst sind und diese richtig anwenden.

Externe Audits

Zusätzlich erfolgt Überprüfung von schützenden Prozessen und deren Anwendung durch externe Unternehmen. In diesem Rahmen werden auch unsere grundlegenden Annahme, welche die Informationssicherheit in unserem Unternehmen betreffen, überprüft.

Informationssicherheit durch technischen Schutz

Systeme

Sämtliche datenverarbeitende Technologie die wir in unserem Unternehmen einsetzen; hierzu zählen unter anderem Workstations, Laptops, Server und Smartphones, Router und Switches aber auch IOT Geräte wie z.B. Drucker, Scanner, Barcodescanner.
Im Besonderen fallen hierunter auch Funkgeräte sowie Repeatertechnik. Auch letztere unterliegen in vollem Umfang unserer Richtlinie für Informationssicherheit.

Systemschutz

Die Spreenauten GmbH schützt die von ihnen verwendeten Systeme durch die strikte Anwendung von technischen Schutz- und Verteidigungsmaßnahmen, die weit über die zugrunde gelegten Richtlinien (-> 3.6) hinausgehen. Diese sind im Dokument “Systemschutz der Spreenauten GmbH (TS)”erläutert.

Office IT Hardware

Unter Office IT Hardware verstehen wir sämtliche lokale Systeme, die unsere Mitarbeiter zur Informationsverarbeitung im Rahmen Ihrer Tätigkeit für die Spreenauten GmbH nutzen. Hierunter fallen unter anderem PC-Systeme, Drucker, Barcodescanner, Smartphones aber auch sämtliche IOT Devices, die bei uns zum Einsatz kommen. Neben der hier formulierten Richtlinie zur Informationssicherheit gelten für diese die Regularien welche im Dokument “IT Sicherheit Spreenauten GmbH: Grundlagen - Schwerpunkt: Devices” (C) zu finden sind.

Anwendungssicherheit

Von uns entwickelte Hard- & Software basiert sicherheitstechnisch jeweils auf unserem “Allgemeinen Sicherheitskonzept der Spreenauten GmbH für die Entwicklung von Hard- & Software” (S) sowie auf einem Sicherheitskonzept, welches individuell abgestimmt ist auf die Funktionalität und die Umgebung in der die Hard- bzw. Software eingesetzt wird. Dieses erweiterte Sicherheitskonzept wird mit dem Kunden erstellt und ist zentraler Bestandteil der regelmäßigen Audits. Zuständig für die Überprüfung der Sicherheitskonzepte für von uns entwickelter Hard- und Software ist der aktuelle CTO welcher wiederum von dem:der aktuellen Informationssicherheits- & Datenschutzbeauftragten zu prüfen ist.

Funktechnik

Die von uns vermietete, verkaufte, installierte, konzeptionierte, entwickelte oder hergestellte Funktechnik unterliegt vollständig unserer Richtlinie zur Informationssicherheit. Im Bereich der Funktechnik wird diese Richtlinie von dem Dokument “Arbeitsanweisung zur Absicherung von Funktechnik welche Kunden von der Spreenauten GmbH zur Verfügung gestellt wird.” (S) Diese Arbeitsanweisung ist für alle Mitarbeiter, die Funktechnik für unsere Kunden konzeptionieren, produzieren und installieren bzw. zur Verfügung stellen, bindend. Die Aktualität und Umsetzung wird engmaschig in internen Audits durch unsere QA überprüft. Sicherheitsmängel werden direkt an den aktuellen Informationssicherheits- & Datenschutzbeauftragten gemeldet. Unser QA bleibt jedoch in der Verantwortung, dass bemängelte Technologie nicht in den

Unser QA bleibt jedoch in der Verantwortung, dass bemängelte Technologie nicht in den Warenverkehr gelangt.

Updates & Patches

Sicherheitsrelevante Updates und Patches der von uns genutzten Systeme werden direkt nach Erscheinen installiert. Spätestens jedoch nach 2h (365 / 24 / 7). Verantwortlich hierfür ist der aktuelle CTO und in dessen Auftrag IT OPS. Die Installation von Updates und Patches sowie die Verantwortlichkeit hierfür bei von uns zur Verfügung gestellter bzw. verkaufter & installierte Funktechnik wird individuell in der jeweiligen Support-Vereinbarung geregelt.
Generell informieren wir unsere Kunden direkt nach Erscheinen, spätestens aber innerhalb von 2h nachdem uns ein relevantes Update oder Patch bekannt wird.

Zentrale Verwaltung

Die von uns betriebenen Systeme werden zentral verwaltet und administriert.
Die Einzelheiten unserer Systemadministration regelt das Dokument “Systemadministration der Spreenauten GmbH” (TS - IT) sowie den darauf basierenden Handlungsanweisungen.

Monitoring

Unsere Systeme werden fortlaufend “live” überwacht. Dies geschieht automatisiert durch standardisierte Systeme z.B. im Rahmen unseres Netzwerk-Monitorings wie auch durch selbst entwickelte Sicherheitsroutinen welche Auffälligkeiten melden. Unser System-Monitoring ist 24/7 durch 2 Mitarbeiter mit weitreichenden Befugnissen, bis hin zum Shut-Down, besetzt.

Ist eine Live-Überwachung aus technischen Gründen nicht möglich, so erfolgt das Auslesen der Logs in regelmäßigen Abständen vor Ort.

Zugrunde liegende Richtlinien
Folgende Richtlinien kommen im Rahmen der Informationssicherheit bei der Spreenauten GmbH zum Tragen:

DSGVO (EU)
Cybersecurity Act (USA)

BSI Standard 200-3 Risikoanalyse basierend auf IT

Siehe hierzu auch:
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf

Unsere Maßnahmen zur Sicherung von Informationen übertreffen diese Richtlinien bei weitem. Wir sehen sie dennoch als Mindestvoraussetzung für die Informationssicherheit in einem Unternehmen an und weisen Ihre Erfüllung jederzeit gerne nach.

Da es sich bei den USA und der EU um unterschiedliche Rechtsräume handelt findet jeweils die Richtlinie Anwendung, die den strengeren Datenschutz fordert.

Interne Audits

Die Überprüfung der von uns getroffenen Maßnahmen hinsichtlich der Informationssicherheit unseres Systems ist zentraler Bestandteil des monatlichen Systemschutz-Audits. Verantwortlich hierfür ist der aktuelle CTO der Spreenauten GmbH. Ferner stellen wir durch automatisierte Surveys (Wissenskontrolle), sicher, dass unsere Mitarbeiter den Zweck der Maßnahmen und die entsprechenden Handlungsanweisung hierfür verinnerlicht haben und anwenden.

Externe Audits

Die Prüfung durch externe Unternehmen ermöglicht es uns, unser Informationssicherheitssystem unter realen Bedingungen (White Hat / Black Hat) zu testen. So Sicherheitsmängel auffallen, werden diese testiert und von uns umgehend beseitigt.

Subsidiarität Informationssicherheit

Kunden

Zum Schutz unserer Kunden, unserer Mitarbeiter:innen und unserem Unternehmen erwarten wir von unseren Kunden die Einhaltung von grundlegenden Standards im Bereich der Informationssicherheit.
Hierzu gehört unter anderem der achtsame Umgang mit Daten, stetige systemweite Prüfung auf Schadsoftware ebenso wie die Verwendung von gesicherter Technologie zum Teilen und zur Verfügung stellen von Daten. Bei der Arbeit vor Ort setzen wir auch hier eine grundlegende Netzwerksicherheit, wie z.B. verschlüsseltes und geschütztes WiFi voraus.

Sollten hier Probleme auftreten, sprechen wir diese direkt bei unseren Kunden an. Sollte sich keine Lösung ergeben und wir das Risikoszenario als für uns bedrohlich einstufen, so behalten wir uns vor Aufträge aus diesem Grund abzulehnen.
Die Mindeststandards für unsere Kunden haben wir in dem Dokument “Informations- & IT-Sicherheitsrichtlinie für Kunden der Spreenauten GmbH” definiert.

Lieferanten

Von unseren Lieferanten erwarten wir gehobene Informationssicherheit. Dies schließt ein vollständiges Protokoll zur Informationssicherheit ebenso ein wie z.B. die Möglichkeit der vollständig verschlüsselten Kommunikation mit AES 256 als Mindeststandard.

Sollten diese Voraussetzungen nicht gegeben sein, so sprechen wir unseren Lieferanten darauf an. Sollte sich hieraus keine Lösung ergeben, so behalten wir uns vor die Geschäftsbeziehung einzustellen bzw. auf Bereiche zu beschränken bei denen kein erweiterter Austausch von Informationen notwendig ist.

Die von uns gegenüber Lieferanten geforderten Standards haben wir im Dokument “Geforderte Standards der Spreenauten GmbH an Lieferanten” (C) definiert. Unter

Absatz 3 sind die Standards zur Informationssicherheit zu finden.

Dienstleister
Für alle unsere Dienstleister gilt ohne Ausnahme die hier vorliegende Richtlinie für Informationssicherheit der Spreenauten GmbH.
Verstöße gegen diese verursachen immer die sofortige Auflösung des Dienstleistungsvertrags.

Behörden

Wir sehen die Lage der Informationssicherheit bei Behörden als kritisch an. Informationen im Bezug auf Dritte geben wir nur dann an Behörden weiter wenn dies von unseren Kunden explizit gewünscht wird - wie z.B. die Beantragung von Frequenzen im Kundenauftrag. Hierfür nutzen wir ausschließlich die originalen Schnittstellen der jeweiligen Behörde. Klassifizierte Daten der Klassen TS, S und C werden nicht an Behörden weitergegeben. Sollte dies dennoch notwendig werden, so ist hierfür die schriftliche Genehmigung des aktuellen CTO UND des aktuellen CEO der Spreenauten GmbH notwendig.

Informationssischerheits- & Datenschutz-Trainings

Um die Umsetzung und Wirksamkeit unserer Informationssicherheitsrichtlinie nebst den hiervon betroffenen grundlegenden Richtlinien zu gewährleisten, trainieren wir unsere Mitarbeiter regelmäßig und prüfen den Erfolg durch interne und externe Audits ab.

Das Training unterliegt den jeweiligen Vorgesetzten. Es findet monatlich statt. Verantwortlich für die Überprüfung des Stattfindens ist der:die aktuelle Informationssicherheits- & Datenschutzbeauftragte der Spreenauten GmbH. Verantwortlich für die Überprüfung des Erfolgs ist der:die aktuelle CTO der Spreenauten GmbH.

Ablauf, Häufigkeit und Ziel des Trainings ist individuell für den jeweiligen Mitarbeiter in unserem HR System geregelt.

Meldung von Verstößen & Problemen

Wir ermutigen unsere Mitarbeiter:innen, Lieferanten:innen und Geschäftspartner:innen jederzeit auf Probleme im Bereich unserer Informationssicherheit hinzuweisen. Für unsere Mitarbeiter:innen haben wir hierfür ein IT-gestütztes System eingerichtet mit dem sie mit nur einem Click Verbesserungsvorschläge äußern und Probleme melden können. Hierfür haben wir zudem ein attraktives Prämiensystem implementiert.

Ansprechpartner:in hierfür ist der aktuelle Informationssicherheits- & Datenschutzbeauftragte.

Whistleblowing

Informationsgeber:innen haben bei uns die Möglichkeit Informationen anonym intern weiterzureichen. Hierzu haben wir ein IT-basiertes System eingerichtet, welches die Identität des Senders effektiv schützt und Anonymität garantiert. Die Spreenauten GmbH garantiert zudem jedem Informationsgeber umfassenden Schutz vor internen Repressalien.

Ansprechpartner hierfür ist der:die aktuelle Informationssicherheits- &-Datenschutzbeauftragte. Auch er:sie wird die Identität des Informationsgebers, soweit ihm diese bekannt wird, anonym halten.

Probleme und Verstöße gegen unsere Datensicherheit werden umgehend bearbeitet und, je nach Grad der Schwere und Komplexität, innerhalb von maximal 2 Wochen behoben. Im Zweifelsfall tritt der Notfallplan der Spreenauten GmbH bei Problemen mit der Informationssicherheit in Kraft. welcher uns erlaubt unsere System & Prozess global teilweise oder ganz zu deaktivieren um die Informationen in unserem Geltungsbereich zu schützen.
Dieser Notfallplan ist im Dokument “Notfallplan der Spreenauten GmbH bei Problemen mit der Informationssicherheit” (S) zu finden.

Überwachung der Informationssicherheit Richtlinie

Die strikte Einhaltung der Informationssicherheitsrichtlinie inklusive Ihrer Unterpunkte wird fortlaufend überwacht, überprüft und ggf. aktualisiert.

Verantwortlich hierfür ist der:die aktuelle Informationssicherheits- & Datenschutzbeauftragte.

Jeder Verbesserungsbedarf wird so schnell wie möglich umgesetzt. Die Mitarbeiter:innen werden ermutigt, ihre Rückmeldung zu dieser Richtlinie zu geben, wenn sie Vorschläge zur Verbesserung der Richtlinie haben. Rückmeldungen dieser Art werden an den:die aktuellen Informationssicherheits- & Datenschutzbeauftragte:n gerichtet.

Änderungen dieser Richtlinie

Diese Richtlinie ist kein Bestandteil eines Arbeitsvertrags mit einem Mitarbeiter der Spreenauten GmbH - wohl aber eine Arbeitsanweisung. Die Spreenauten GmbH kann sie jederzeit ändern um die Informationssicherheit in Ihrem Unternehmen zu aktualisieren bzw. zu verbessern.

Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Richtlinie unwirksam oder undurchführbar sein oder unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Richtlinie im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der Zielsetzung (Informationssicherheit) am nächsten kommen, welche mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Richtlinie als lückenhaft erweist.