



selbst & bewusst

Tipps für den persönlichen Datenschutz bei Facebook

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Angemeldet bleiben[Passwort vergessen?](#)

Du ziehst weiter? Bleibe in Verbindung
Besuche facebook.com auf deinem Handy.

[Hol dir Facebook-Handy](#)

Registrieren

Facebook ist und bleibt kostenlos.

Vorname: Nachname: Deine E-Mail-
Adresse: E-Mail nochmals
eingeben: Neues Passwort:

Ich bin:

Geschlecht auswählen: Geburts-
tag:Tag: Monat: Jahr:

Warum muss ich meinen Geburtstag angeben?

Wenn du auf „Registrieren“ klickst, akzeptierst du unsere Nutzungsbedingungen und erklärst unsere Datenverwendungsrichtlinien sowie Bestimmungen zur Verwendung von Cookies gelesen zu haben.

[Erstelle eine Seite für eine Berühmtheit, eine Band oder ein Unternehmen.](#)

Eintritt frei?

Soziale Netzwerke im Internet spielen eine große Rolle für die Kommunikation und die Pflege von Freundschaften. Dabei darf sich der Nutzer nicht der Illusion hingeben, dass ihm dies völlig kostenlos zur Verfügung gestellt wird. Die Währung, mit der die Mitgliedschaft bezahlt wird, sind die eigenen persönlichen Daten. Man erlaubt Facebook, diese Daten zu sammeln und sie für eigene Zwecke zu verwenden. Über diesen Umstand sollte sich jeder Nutzer bewusst sein und stets abwägen, welche Informationen zur eigenen Person er oder sie tatsächlich preisgeben möchte. Welche privaten Gewohnheiten, welche persönlichen Vorlieben, welche Aspekte der Freizeitgestaltung und des Konsumverhaltens sollen für wen veröffentlicht werden?

Wir haben in dieser Broschüre einige Tipps und Hinweise für die Nutzung von Facebook als weltweit größtes soziales Netzwerk zusammengestellt, die dem Nutzer ermöglichen, weitgehend den Selbstschutz zu wahren. Dies ist schwer genug, da die Nutzungs- und Datenschutzbestimmungen und die Privatsphäre-Einstellungen nicht immer verständlich sind. Doch selbst bei sorgfältig gewählter Konfiguration sind Daten, die einmal im Internet veröffentlicht wurden, nicht mehr kontrollierbar und finden vielleicht ungewollte Verbreitung. Denn jeder der Freunde kann die Inhalte ins freie Internet stellen und damit einem unbegrenzten Personenkreis zugänglich machen. Diese Broschüre und die darin enthaltenen Einstellungstipps können nicht Ihren gesunden Menschenverstand ersetzen. Fragen Sie sich daher vor jeder Veröffentlichung, ob Sie davon auch wildfremden Menschen auf der Straße erzählen würden. Wenn nicht, sollten Sie diese Information auch nicht verbreiten, denn sie könnte sich als unliebsamer Bumerang erweisen.

Mobile Nutzung

Die App bietet nicht alle Einstellmöglichkeiten

Viele Facebook-Mitglieder nutzen das Netzwerk von ihrem Mobiltelefon aus, über die sog. „Facebook-App“. Diese bietet jedoch nicht alle Funktionalitäten und Einstellmöglichkeiten, die auf der Webseite von Facebook verfügbar sind. Die nachfolgenden Tipps beziehen sich vorrangig auf die Webseite. App-Nutzer können auf dem Mobiltelefon nicht verfügbare Privatsphäre-Einstellungen über die Facebook-Internetseite vornehmen.

1 Mein Name ist Nobody

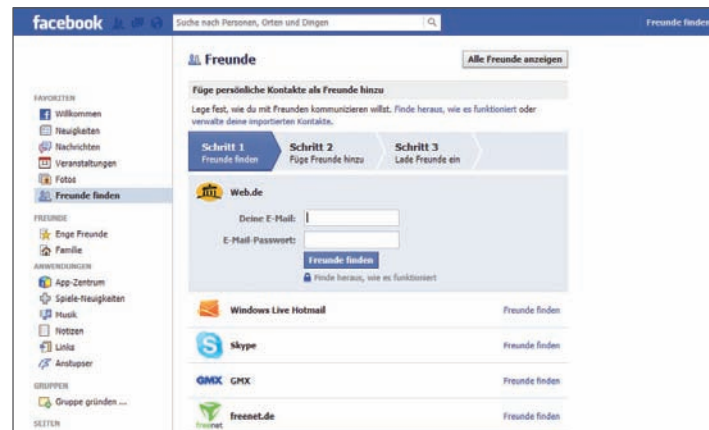
Benutzung von Pseudonymen oder Nicknames

Wer nicht von jedermann mit seinem Echtnamen bei Facebook oder über Suchmaschinen gefunden werden möchte, sollte sein Profil unter einem Pseudonym (bzw. Nickname) anlegen oder zumindest den Nachnamen verschleiern. Das Recht dazu ist im Gesetz festgeschrieben. Die Nutzungsbedingungen von Facebook, die auf Angabe des wahren Namens bestehen, sind daher unwirksam. Sollte Facebook trotzdem das Profil wegen der Pseudonym-Verwendung vorläufig sperren, müssen Sie für sich entscheiden, ob Sie Ihren Account mit Ihrem richtigen Namen fortführen wollen. Wir werden uns weiter dafür einsetzen, dass Facebook das Recht auf eine pseudonyme Nutzung anerkennt.

2 Automatische Freunde

Die Option „Freunde finden“

Nach Erstellen eines neuen Profils erscheint das Angebot, Facebook auf das eigene E-Mail-Postfach oder das Adressbuch zugreifen zu lassen, um Freunde zu finden. Dabei werden private Daten von Dritten (die Adressen Ihrer E-Mail-Kontakte) an Facebook übertragen und dort gespeichert. Da damit sicherlich nicht jeder Ihrer Freunde und Bekannten einverstanden ist, lehnen Sie dieses Angebot ab und laden Sie Freunde bei Facebook lieber individuell ein.



3 Nackt ins Netz?

Die Privatsphäre-Einstellungen



Unter den „**Privatsphäre-Einstellungen**“ kann die grundsätzliche Einstellung für Beiträge oder Veröffentlichungen bei Facebook festgelegt werden. Dies betrifft vor allem die Nutzer der Facebook-App. In den meisten Fällen ist die Option „Freunde“ passend. In bestimmten Fällen sollte jedoch die Möglichkeit genutzt werden, die Sichtbarkeit auf einzelne Personen oder Freundeslisten zu begrenzen („Benutzerdefiniert“). Die Einstellung „Freunde von Freunden“ hingegen ist weitreichender als sie klingt: bei durchschnittlich 130 Freunden hat ein normaler Facebook-Nutzer weit über 10.000 „Freunde von Freunden“, die ihm größtenteils unbekannt sind und auf deren Auswahl er keinen Einfluss hat. Jede dieser Personen

kann einsehbare Informationen nach Belieben verwenden oder weitergeben. Diese Einstellung unterscheidet sich daher kaum von einer Freigabe für die Öffentlichkeit.

4 Ungooglebar

Das eigene Profil vor Suchmaschinen und anderen Neugierigen schützen

Um zu verhindern, dass das eigene Facebook-Profil mit einer detaillierten Vorschau in Suchmaschinen landet, ist Umsicht und eine zusätzliche Sicherheitseinstellung nötig. Wichtig ist, dass unter

- > „**Privatsphäre-Einstellungen**“
- > „**Wer kann nach mir suchen?**“
- > „**Möchtest du, dass andere Suchmaschinen einen Link zu deiner Chronik enthalten?**“
- > „**Bearbeiten**“

das eventuell gesetzte Häkchen entfernt wird. Allerdings lässt sich auch mit dieser Einstellung nur schwer verhindern, dass der eigene Name irgendwann von einer Suchmaschine erfasst wird. Beispielsweise über einen hinterlassenen Kommentar auf einer Fanseite oder auf dem öffentlich einsehbaren Profil eines Freundes. Dieses Risiko sollten vor allem Personen mit seltenen Namen bedenken und ihr Konto besser unter einem Pseudonym anlegen (siehe Tipp1).



Eine weitere Möglichkeit, wie das eigene Profil von Dritten gefunden werden kann, ist über die E-Mail-Adresse oder eine bei Facebook hinterlegte Telefonnummer. Deren Auffindbarkeit kann über

- > „Privatsphäre-Einstellungen“
- > „Wer kann nach mir suchen?“
- > „Wer kann dich anhand der von dir angegebenen E-Mail-Adresse oder Telefonnummer finden?“
- > „Bearbeiten“



gesteuert werden. Hier sollte auf „Freunde“ eingeschränkt werden. Grundsätzlich empfiehlt sich als Basis für die Facebook-Anmeldung die Nutzung einer separaten und nicht allgemein bekannten E-Mail-Adresse.

5 Strip Poker ... Zugriff von Anwendungen, Spielen und Webseiten

Vielen Facebook-Nutzern ist nicht bewusst, dass auch die sogenannten „Apps“, also Anwendungen, Spiele, aber auch Webseiten, auf ihre persönlichen Daten zugreifen. Dabei müssen nicht einmal Sie selbst diese Apps nutzen, es reicht schon, wenn ein Freund von Ihnen es tut und Sie diese Funktion nicht unterbunden haben. Diese wichtigen Einstellungen verbergen sich unter

- > „Privatsphäre-Einstellungen“
- > „Anwendungen“
- > „Von anderen Nutzern verwendete Anwendungen“
- > „Bearbeiten“



Hier können Sie prüfen und festlegen, welche Profildaten dem Zugriff durch Apps und Webseiten, die von Freunden genutzt werden, offen stehen. Wollen Sie überhaupt keine Anwendungen oder Apps nutzen, sollten Sie unter

- > „Privatsphäre-Einstellungen“
- > „Anwendungen, die du verwendest“
- > „Bearbeiten“

die Anwendungsplattform komplett deaktivieren. Damit unterbinden Sie gleichzeitig die Weitergabe der eigenen Daten über Freunde oder Anwendungen.

6 Umsonst mit meinem Namen Eigene Daten in Werbeanzeigen



Haben Sie sich vielleicht schon einmal darüber gewundert, dass einer Ihrer Facebook-Freunde plötzlich in einer Werbeanzeige auftaucht? Das liegt daran, dass diese Freunde Facebook die Erlaubnis erteilt haben, die eigenen Daten für Werbeanzeigen zu verwenden. Wenn Sie gegenüber Ihren Freunden nicht als Werbeträger benutzt werden möchten, können Sie unter „**Privatsphäre-Einstellungen**“ die Verwendung Ihrer Daten in „**Werbeanzeigen**“ unterbinden.

7 Deine Daten in meiner Hand Umgang mit den persönlichen Daten Dritter

Wer Fotos oder Videos von Partys, Familienfeiern u. ä. zu Facebook hochlädt, muss vorab sicherstellen, dass die darauf abgebildeten Personen mit der Veröffentlichung einverstanden sind. Dies gilt auch für Bilder in „privaten“ Fotoalben. Übrigens: Auch die Eingabe von E-Mail-Adressen oder Handy-Nummern bei Facebook zum Zweck der Freundesuche sollte nur erfolgen, wenn die betroffenen Personen mit der Weitergabe ihrer persönlichen Daten einverstanden sind. Denn auch solche Informationen werden von Facebook gespeichert. Berufliche Kontakte sollten niemals über Facebook verwaltet werden. Auch ein nicht rein privat genutztes Smartphone sollte nicht mit Facebook synchronisiert werden (siehe Punkt 2).

8 Dein Leben – ein offenes Buch? Regelmäßig die Chronik aufräumen!

Mit der „Chronik“ hat Facebook eine neue Darstellung des Profils eingeführt. Hierüber kann schnell und einfach in die Vergangenheit eines Mitgliedes gescrollt werden. So können zum einen alte und längst vergessene Veröffentlichungen wieder ans Licht kommen. Es lässt sich auch für Dritte leicht nachvollziehen, was Sie zu einem bestimmten Zeitpunkt in der Vergangenheit interessiert hat oder mit wem Sie damals in engerer



Verbindung standen. Daher sollten Sie gelegentlich das Profil aufräumen. Dies geht übergreifend über

-> „Privatsphäre-Einstellungen“

-> „Möchtest du das Publikum für Beiträge einschränken, die du mit Freunden von Freunden oder öffentlich geteilt hast“

-> „Vergangene Beiträge einschränken“

Hiermit werden alle alten Beiträge pauschal so eingeschränkt, dass nur noch die eigenen Freunde sie einsehen können. Sie können in Ihrer eigenen Chronik und dem Aktivitätenprotokoll aber auch bei jedem alten Beitrag direkt (sog. „inline“) nachträglich die Sichtbarkeit ändern oder ihn rückwirkend löschen.

Grundsätzlich sollte man gut überlegen, inwieweit man die eigene Vergangenheit in der Chronik offenlegt. Persönliche Highlights wie eigene Babyfotos, der erste Kuss, der Hochzeitstag oder die Geburt der Kinder werden so einer breiten Öffentlichkeit zugänglich gemacht.

9 Sicher ist sicher

Sichere Netzwerkverbindung



Um den Zugang zu Facebook sicher zu halten und das Ausspähen der eigenen Daten durch Dritte zu erschweren, sollte Facebook nur über verschlüsselte Netzwerkverbindungen genutzt werden. Hierzu muss das Häkchen gesetzt sein unter

-> „Kontoeinstellungen“

-> „Sicherheit“

-> „Sicheres Durchstöbern“

-> „Bearbeiten“

Ob Sie eine sichere Verbindung nutzen, erkennen Sie durch einen Blick auf die Adressleiste Ihres Web-Browsers. Dort sollte am Anfang „https://“ stehen, auch schon beim Aufruf der Facebook-Anmeldeseite.

10 Tag der offenen Tür?

Empfänger für Beiträge und Einladungen

Für jeden Beitrag bei Facebook sollten Sie festlegen, an wen er sich richtet. Der Kreis der Empfänger lässt sich über das Feld „Privatsphäre“ einstellen. Vor allem Einladungen zu Veranstaltungen, Partys oder Treffen sollten nur an erwünschte Gäste versandt werden. Wird eine Veranstaltung als „öffentlich“ markiert, kann der Termin von jedem weiterverbreitet werden und ist nicht mehr zu kontrollieren.



11 Nicht alle Kekse schmecken

Löschen von Cookies

Cookies sind kleine Dateien, die von Webseiten auf Ihrem Rechner gespeichert werden, um Sie beispielweise als Seitenbesucher wiederzuerkennen. Auch Facebook setzt Cookies ein und kann u. a. in Verbindung mit dem „Gefällt mir“-Button die Mitglieder auf entsprechenden Webseiten verfolgen und das Surfverhalten außerhalb Facebooks erfassen. Bei den meisten Webseiten ist es übrigens unerheblich, ob Sie auf den „Gefällt mir“-Button klicken oder nicht - bereits der Aufruf einer solchen Seite wird von Facebook erkannt. Auch wer kein Mitglied von Facebook ist, erhält beim Besuch von Facebook Fan-Pages ein Cookie, über das ihn Facebook fortan im Netz wiedererkennen kann. Den besten Schutz davor bietet das regelmäßige Löschen der Cookies im Menü Ihres Web-Browsers. Häufig können dort auch die aktuell vorhandenen Cookies eingesehen werden.

12 Vor dem Spiegel

Selbstauskunft bei Facebook



Facebook bietet die Möglichkeit, eine Kopie des eigenen Profils herunterzuladen. Dies geht über den Link am unteren Ende der Seite

-> „*Kontoeinstellungen*“

-> „*Lade eine Kopie deiner Facebook-Daten herunter*“

Neben dem normalen Archiv ist hier vor allem die Option „**Erweitertes Archiv**“ interessant. Dieses enthält zusätzlich zu den selbst erstellten Inhalten umfangreiche Daten, die Facebook intern über Sie anlegt und speichert. Beispielsweise den Zeitpunkt jeder einzelnen Anmeldung und des dabei von Ihnen genutzten Computers (IP-Adresse, Web-Browser und zugeteilte Cookies). Auch ist

erkennbar, dass jeder Klick auf Werbeanzeigen protokolliert wird, ebenso bleiben gelöschte Freundschaften bei Facebook weiterhin gespeichert.

All diese Daten ermöglichen eine umfassende Rekonstruktion der Facebook-Nutzung und geben tiefe Einblicke in Vorlieben, Verhalten oder Aufenthaltsorte eines Mitglieds. Facebook nutzt und analysiert diese Informationen, um ein immer umfangreicher werdendes Persönlichkeitsprofil zu jedem Mitglied aufzubauen.

13 Captured!

Was tun wenn die eigene Identität missbraucht wird?

Bei Facebook können Profile mit beliebigen Namen angelegt werden. So kann eine Person ohne ihr Wissen bei Facebook angemeldet sein, weil ein Dritter ein Konto unter ihrem Namen angelegt hat. Sofern es sich nicht um eine einfache Namensgleichheit handelt, ist es wichtig, schnell und richtig zu reagieren!

Das betreffende Profil sollte Facebook umgehend zur Löschung gemeldet werden. Hierzu gibt es bei jedem Profil bei Klick auf das Symbol neben „Nachricht senden“ die Option „Melden/Blockieren“. Im darauf folgenden Menü markiert man „Diese Chronik gibt vor, eine andere Person zu sein oder ist eine Fälschung“ und folgt den weiteren Anweisungen.

Sind Sie selbst kein Facebook-Mitglied, erhalten Sie im Facebook „Hilfe“-Bereich nach Eingabe von Suchbegriffen wie „missbrauch melden“ Hinweise für das weitere Vorgehen.

Zur Überprüfung der Identität verlangt Facebook eine Kopie oder einen Scan bzw. Fax des Personalausweises. Hier sollte man keine unnötigen Daten offenlegen. Empfehlenswert ist, zunächst eine Kopie des Ausweises anzufertigen und dort alle nicht relevanten Informationen wie Adresse, Ausweisnummer, weitere Vornamen, Geburtsort, Augenfarbe oder Körpergröße zu schwärzen. Das bearbeitete Dokument wird anschließend erneut kopiert und die Kopie eingescannt und an Facebook übermittelt.

14 Spurlos verschwunden?

Tipps für die Abmeldung von Facebook

Unter „Kontoeinstellungen“ bietet Facebook zwar eine Option zum Deaktivieren des Kontos, dies ist jedoch keine endgültige Kündigung. Das Profil wird nur stillgelegt und alle Daten bleiben vollständig und zeitlich unbegrenzt erhalten. Wer Facebook dauerhaft verlassen will, muss eine spezielle Kündigungsseite aufsuchen. Diese finden Sie am schnellsten, indem Sie im Facebook „Hilfe“-Bereich den Begriff „kündigen“ eingeben oder über den Direkt-Link:



https://www.facebook.com/help/delete_account

WICHTIG! Vor der Kündigung sollten Sie Ihr Profil aufräumen und leeren.

- Das heißt:
- Entfernen aller Angaben zu Person und Interessen (oder Ersetzen durch belanglose Daten)
 - Aufräumen der Chronik
 - Löschen aller Nachrichten
 - Löschen des Profilfotos und Auflösen aller Fotoalben
 - Leeren der Freundesliste
 - Auflösen von Gruppenmitgliedschaften

Facebook ist nach dem Gesetz zwar verpflichtet, gelöschte Daten tatsächlich zu vernichten. In den Nutzungsbedingungen ist jedoch eine Speicherung von Daten über das Ende der Mitgliedschaft hinaus vorbehalten. Eine Garantie für die restlose Löschung von Profilen gibt es nicht, daher sollten Sie möglichst wenig Daten von Ihnen zurücklassen.



Wussten Sie übrigens...

Zum Schluss noch ein paar Hinweise und Denkanstöße

- ... dass der einfachste Weg vor einer umfassenden Verfolgung des eigenen Surfverhaltens im Internet darin besteht, für Facebook einen separaten Web-Browser zu verwenden? Auf vielen PCs sind neben dem Internet Explorer auch Firefox oder Opera installiert. Durch den Extra-Browser nimmt die Verfolgbarkeit der „normalen“ Internetnutzung durch Facebook stark ab.
- ... dass jeder andere Facebook-Nutzer Ihre eigene Freundesliste nachvollziehen kann, sobald er Ihnen eine Freundschaftsanfrage schickt? Solange Sie eine Anfrage nicht ablehnen, erscheinen dem Anfrager bereits Personen aus Ihrer Freundesliste unter „Personen, die du vielleicht kennst“. Damit kann ein Profil in gewissem Umfang ausgespäht werden. Seien Sie daher vorsichtig bei Anfragen unbekannter Personen und lehnen Sie diese im Zweifel schnellstmöglich ab!
- ... dass die eigenen Profile bei verschiedenen sozialen Netzwerken oder Webseiten sehr einfach zusammengeführt werden können, wenn überall das gleiche Benutzerbild bzw. Profilfoto verwendet wird? Über Bildersuchmaschinen, z. B. von Google, werden damit Profile auffindbar, auch wenn sie unter Pseudonym angelegt sind. Daher für jedes Benutzerprofil stets ein anderes Bild verwenden.

- ... dass Fotos von Digitalkameras oder Mobiltelefonen häufig sog. „Geo-Daten“ enthalten, d.h. die genauen geografischen Daten des Aufnahmeortes? So kann z.B. über ein hochgeladenes Foto aus dem heimischen Garten von Dritten (und von Facebook) eventuell die eigene Wohnadresse bestimmt werden. Um sich davor zu schützen, sollten Sie die Standorterfassung bei Digitalkameras oder Smartphones ausschalten. Oder Sie überarbeiten Fotos vor der Veröffentlichung und entfernen dabei die sog. „Metadaten“, in vielen Bildbearbeitungsprogrammen auch „EXIF-Daten“ genannt.
- ... dass sich Facebook in den Nutzungsbedingungen das Recht einräumt, private Chats nach Schlagworten oder auffälligen Mustern zu durchsuchen? Im Klartext: Die private Kommunikation wird belauscht. Ziel ist die Aufdeckung von Annäherungsversuchen Erwachsener an Minderjährige - ein durchaus ehrenhaftes Anliegen. Jedoch ist jede Überwachung privater Kommunikation datenschutzrechtlich bedenklich, da - sobald einmal eingerichtet - diese leicht für andere Zwecke missbraucht werden kann.
- ... dass Facebook sich eine sehr weitgehende Eigennutzung für Veröffentlichungen der Mitglieder einräumt? Zitat aus den Nutzungsbedingungen (gültig seit 11.12.2012): „Du gibst uns eine nicht-exklusive, übertragbare, un-terlizenzierbare, gebührenfreie, weltweite Lizenz zur Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammen- hang mit Facebook postest („IP-Lizenz“). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.“ So können von Nutzern hochgeladene Informationen wie Fotos oder Texte (von Facebook „IP-Inhalte“ genannt) von Facebook für eigene Zwecke z.B. als Werbemotiv eingesetzt werden.
- ... dass Internet-Recherchen zu Bewerbern bei Arbeitgebern oder Vermietern heutzutage durchaus üblich sind? Vor allem bei Kindern und Jugendlichen wirken Facebook-Einträge oft auch in ihre Zukunft: Partybilder, Peinlichkeiten oder andere kompromittierende Inhalte aus der Kindheit oder Jugendzeit können sich später negativ auf die Ar- beitsplatz- oder Wohnungssuche auswirken. Hier kommt Eltern und gerade auch Schulen die besondere Rolle zu, Kinder und Jugendliche über die Dauerhaftigkeit von Daten und Spuren im Internet aufzuklären.

Zu guter Letzt...

Die hier zusammengestellten Hinweise entsprechen dem aktuellen Stand (Januar 2013), aber eine gedruckte Broschüre wie diese kann unmöglich mit den rasanten Veränderungen im Inter- net mithalten. Bitte überprüfen Sie von Zeit zu Zeit, welche Features Facebook für die Privatsphä- re-Einstellungen anbietet. Bei neuen oder veränderten Einstellungsmöglichkeiten sollten Sie Ihre individuellen Einstellungen anpassen. Kontrollieren und aktualisieren Sie Ihre Privatsphäre- Einstellungen regelmäßig, denn Ihre eigene Verantwortlichkeit kann Ihnen niemand abnehmen.



Diese Broschüre ist auch online als PDF-Datei verfügbar unter www.datenschutz-hamburg.de.

Herausgeber:

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Klosterwall 6

20095 Hamburg

Tel.: 040/42854-4040 (Geschäftsstelle)

Fax: 040/42854-4000

E-Mail: mailbox@datenschutz.hamburg.de

Layout: KAMEKO Design Gbr

Titelbild: Thomas Krenz

Druck: Print 74

Diese Publikation kann auch unter www.datenschutz-hamburg.de im PDF-Format heruntergeladen werden.

In Zusammenarbeit mit:



Behörde für Schule und Berufsbildung

SchulInformationszentrum (SIZ)

Hamburger Straße 125a, 22083 Hamburg

Tel.: 040. 428 99 22 11

Tel.: 040. 428 63 27 28

schulinformationszentrum@bsb.hamburg.de

www.hamburg.de/siz