SOCIAL MEDIA LEITLINIE

DES PRÄSIDIUMSARBEITSKREISES „DATENSCHUTZ UND IT-SICHERHEIT“
DER GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

Inhalt

Präambel

Das Handeln von Informatikerinnen und Informatikern steht in Wechselwirkung mit unterschiedlichen Lebensweisen, deren besondere Art und Vielfalt in Social Media in herausragender Weise zum Ausdruck zukommt.

In der Nutzung von Social Media liegen einerseits besondere Chancen, sich mit kommunikativem Handeln darzustellen und u.a. den Diskurs über relevante Fragen der Informatik in der Öffentlichkeit zu befördern. In der Entwicklung von Social Media liegen aufgrund der Dichte und Sensitivität der hierbei anfallenden personenbezogenen Daten aber auch besondere Risiken für die informationelle Selbstbestimmung.

Neben allgemeinen moralischen Prinzipien wie beispielsweise in der Deklaration der Menschenrechte und im Recht auf informationelle Selbstbestimmung festgeschrieben müssen für Informatikerinnen und Informatiker auch die Ethischen Leitlinien der Gesellschaft für Informatik e.V. (GI) als relevanter Maßstab bei der Entwicklung und Nutzung von Social Media einbezogen werden.

Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik e.V. (GI) will mit dieser Leitlinie eine Orientierung bereitstellen, um die Integration berufsethischer Aspekte sowohl in der Nutzung von Social Media als auch in der Entwicklung entsprechender Plattformen zu fördern.

I. Social Media Verständnis

Bereits heute verbindet das Internet mehr als ein Drittel der Weltbevölkerung. Ein besonderes Medium im Internet stellen Social Media dar, die es Menschen weltweit ermöglichen, sich untereinander zu vernetzen, auszutauschen und Inhalte einzeln oder in Gemeinschaft zu erstellen und zu veröffentlichen. Auf der Basis von Social Media entstehen Gemeinwesen, die allerdings nicht nach öffentlichem, sondern nach privatem Recht organisiert sind. Mehr als 40% der Internetnutzer setzen Social Media vor allem zur Selbstdarstellung mit hoher Reichweite und geringem Einsatz ein.

Genau deshalb sind Social Media auch für Fachgesellschaften interessant: Man kann Mitteilungen mit einem geringen Aufwand in einem riesigen Netzwerk verteilen, auf anderen Wegen kaum ansprechbare Zielgruppen erreichen und direktes Feedback von Mitgliedern und Interessenten entgegennehmen.

Neben diesen Chancen gibt es aber eine Reihe von Risiken. Vielen widerstrebt es, dass zentrale Infrastruktur-Aufgaben von privaten Unternehmen wahrgenommen werden, ohne dass diese einer verantwortlichen Regulierung durch eine gewählte Exekutive unterliegen. Hier sind die nationalen Regierungen und natürlich auch die EU dringend gefragt.

Des Weiteren widersprechen Social Media dem Prinzip der dezentralen Vernetzung: Alle Daten werden zentral beim Social Media Betreiber gespeichert. Dabei werden relevante Dienste der Social Media Plattform den Nutzern dem Anschein nach „kostenlos“ bereitgestellt, in Wahrheit aber von den Nutzern mit deren Daten „bezahlt“, die der Anbieter zwecks Gewinnerzielung nutzt. Die mit der zentralen Speicherung der Daten sowie mit der Monetarisierung verbundenen Risiken für das informationelle Selbstbestimmungsrecht sind vielen Benutzerinnen und Benutzern nicht bewusst.

Erschwerend kommt hinzu, dass bei der Entwicklung mancher Social Media Plattform aus Sicht des Präsidiumsarbeitskreises relevante Prinzipien vernachlässigt werden und die vermeintlich private Kommunikation im Freundeskreis oft sehr viel öffentlicher ist als von der Benutzerin oder dem Benutzer gedacht, und oftmals auch keinerlei Schutz der teilweise sensitiven Daten gegen anlasslose Massenüberwachung bereitgestellt wird.

Aus diesen Gründen sollten Social Media nur mit entsprechender Sorgfalt genutzt werden. Vor der Nutzung einer spezifischen Social Media Plattform ist eine Prüfung geboten, in welchem Grad diese die aus der Sicht des Präsidiumsarbeitskreises relevanten Kriterien erfüllt. Änderungen der Nutzungsbedingungen einer Social Media Plattform können unter Umständen eine erneute Prüfung mit anschließender Neubewertung erforderlich machen.

Bei Social Media Plattformen, die im Rahmen einer solchen Prüfung relevante Zweifel hinterlassen, kann je nach Ausprägung des Zweifels eine der folgenden Formen der digitalen Abstinenz angezeigt sein: Bei der bedingten Form der Abstinenz wird auf der betreffenden Social Media Plattform nur gepostet, was auch öffentlich sein darf bzw. soll. Aus Sicht des Präsidiumsarbeitskreises wären dies z.B. Verweise auf eigene Pressemitteilungen oder Blogeinträge, Lese-Empfehlungen oder Veranstaltungseinladungen. Bei Zweifeln im Hinblick auf die Verträglichkeit der Social Media Plattform mit dem Image der GI kann von der unbedingten Form der Abstinenz Gebrauch gemacht werden, bei der auch vom Posten öffentlicher Informationen Abstand genommen und die Social Media Plattform grundsätzlich gemieden wird. In Fällen, in denen eine bestimmte Social Media Plattform wiederholt, nachweislich und eklatant gegen relevante Prinzipien verstößt, kann die besondere Form der Abstinenz angezeigt sein.

Mit dieser Herangehensweise möchte der Präsidiumsarbeitskreis einen Beitrag zur Handhabung der besonderen Chancen und Risiken bei Social Media leisten, der es ermöglicht, sowohl das entsprechende Potenzial auszuschöpfen, aber auch über relevante Risiken aufzuklären. Parallel hierzu möchte der Präsidiumsarbeitskreis Informatikerinnen und Informatiker, die an der Entwicklung von Social Media beteiligt sind, zur konstruktiven Berücksichtigung datenschutzrelevanter Prinzipien ermutigen.

Somit wird sowohl im Hinblick auf Nutzung als auch auf Entwicklung von Social Media der Diskurs um den verantwortungsvollen Umgang mit Informationstechnik gefördert. Der Präsidiumsarbeitskreis lädt jeden herzlich dazu ein, sich daran zu beteiligen.

II. Bewertungskriterien für Social Media

Vor der Nutzung relevanter Social Media Plattformen ist eine Prüfung der Plattform und des dahinterstehenden Anbieters geboten, die neben üblichen Kriterien wie Funktionalität, Erreichbarkeit spezifischer Zielgruppen usw. auch Grundsätze aus der Datenschutz-Richtlinie der OECD und Prinzipien aus den Ethischen Leitlinien der GI beinhalten sollte.

A. Grundsatz der Begrenzten Datenerhebung

Bei der Erhebung personenbezogener Daten sind Grenzen zu setzen. Die Erhebung solcher Daten muss verhältnismäßig sein und sollte mit Wissen bzw. Einwilligung des Betroffenen erfolgen. Eine Datenerhebung mit unrechtmäßigen oder unlauteren Mitteln ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

B. Grundsatz der Datenqualität

Personenbezogene Daten müssen ihrer Zweckbestimmung entsprechen und in dem für diesen Zweck nötigen Ausmaß genau, vollständig und aktuell sein. Eine Nutzung von falschen Daten oder gar deren absichtliche Verfälschung mit Auswirkungen auf die Rechte und Interessen der Betroffenen ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

C. Grundsatz der Zweckbestimmung

Der Zweck, für den die personenbezogenen Daten erhoben werden, ist zum Zeitpunkt der Datenerhebung festzulegen. Die spätere Nutzung ist auf die Erfüllung dieses Zwecks bzw. sonstiger Zwecke zu beschränken, vorausgesetzt, diese Zecke sind mit den ursprünglichen Zwecken nicht unvereinbar und werden bei jeder Änderung der Zweckbestimmung angegeben. Unspezifische oder mehrdeutige Zweckbestimmungen sind aus Sicht des Präsidiumsarbeitskreises inakzeptabel (insbesondere wenn der Betroffene darin enthaltene unerwünschte Zwecke nicht ausschließen kann).

D. Grundsatz der Nutzungsbegrenzung

Die Nutzung von personenbezogenen Daten ist auf den ursprünglichen Zweck beschränkt. Eine Offenlegung, Bereitstellung oder anderweitige Nutzung für einen anderen als den ursprünglich angegebenen Zweck ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel (es sei denn, dies geschieht mit Einwilligung des Betroffenen oder von Gesetzes wegen).

E. Grundsatz der Sicherung

Personenbezogene Daten sind durch angemessene Sicherheitsvorkehrungen gegen Risiken wie Verlust sowie Zugang, Zerstörung, Nutzung, Veränderung oder Offenlegung der Daten durch Unbefugte zu sichern. Fehlende Verschlüsselung, fehlende Multifaktor-Authentifizierung und andere nicht dem Stand der Technik entsprechende Sicherungsmaßnahmen sind aus Sicht des Präsidiumsarbeitskreises nicht akzeptabel.

F. Grundsatz der Offenheit

Bezüglich Entwicklungen, Vorgehensweisen und Maßnahmen im Hinblick auf personenbezogene Daten ist generell eine Politik der Offenheit gegenüber den Betroffenen zu demonstrieren. Es ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel, wenn für den Betroffenen das Vorhandensein und die Art personenbezogener Daten, ihre Hauptverwendungszwecke sowie die Identität und das Domizil der verantwortlichen Stelle nicht einfach festzustellen sind.

G. Prinzip der Fach- und Sachkompetenz

Fachkompetenz nach dem Stand von Wissenschaft und Technik sowie die Bereitschaft, die Rechte und Interessen der Betroffenen zu wahren, sind aus Sicht des Präsidiumsarbeitskreises relevante Merkmale eines empfehlenswerten Social Media Anbieters. Hierzu gehört auch, die Veränderungen an der Plattform so zu planen und vorzunehmen, dass alle Nutzer sich darauf einstellen und ihre Interessen vertreten können. Das versteckte Platzieren von für den Betroffenen relevanten Datenschutzfunktionen und/oder deren unnötig komplexe Gestaltung sind aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

H. Prinzip der Rechts- und Datenschutzkompetenz

Die Kenntnis und Wahrung der einschlägigen rechtlichen Regelungen, etwa zum Daten- und Persönlichkeitsschutz und Urheberrecht sind aus Sicht des Präsidiumsarbeitskreises relevante Merkmale eines empfehlenswerten Social Media Anbieters. Dies gilt besonders, wenn er sich Neuerungen von

Nutzern genehmigen lässt. Hier ist den Nutzern z.B. klar zu erläutern, welche Informationen der Anbieter durch die Genehmigungen erhält und welche Nutzungsmöglichkeiten sich ihm erschließen. Einseitige und ggf. nicht mit einschlägigen Gesetzen im Einklang stehende Willenserklärungen des Anbieters sowie undurchsichtige bzw. unverständliche Datenschutzerklärungen sind aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

I. Prinzip der Mitarbeiterbeteiligung

Die Beteiligung von Mitarbeiterinnen und Mitarbeitern im Hinblick auf den verantwortungsvollen Einsatz von Informationstechnik einschließlich der Entwicklung ethischer Kriterien, langfristiger gesellschaftlicher Akzeptanz und Nachhaltigkeit ist ein aus Sicht des Präsidiumsarbeitskreises relevantes Merkmal eines empfehlenswerten Social Media Anbieters. Die Gestaltung von technischen Möglichkeiten zur einseitigen wirtschaftlichen Verwertung von Daten unter Missachtung des Rechts auf informationelle Selbstbestimmung ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

J. Prinzip der Nutzerbeteiligung

Die Bereitschaft, die Nutzer an der Gestaltung der Plattform und ihrer Nutzungsbedingungen angemessen zu beteiligen, ist ein aus Sicht des Präsidiumsarbeitskreises relevantes Merkmal eines empfehlenswerten Social Media Anbieters. Nichtbeachtung wesentlicher Anforderungen des Verbraucherschutzes (z.B. Auswertung oder Überwachung des Verhaltens der Nutzer ohne deren angemessene Beteiligung) ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

K. Prinzip der selbstbestimmten Nutzung

Der Nutzer als Akteur muss den Darstellungsgrad seiner Identität selbst bestimmen können, d.h. mit pseudonymisierten Zugängen ohne direkten Personenbezug. Rein konsumptive Nutzung muss sogar anonym möglich sein. Jeder Nutzer kann mit unterschiedlichen Profilen aktiv werden, ohne dass eine Verknüpfung der Profile erfolgt. Der Akteur hat ein Recht, das Nutzungsrecht an seinen bereitgestellten Information zu begrenzen (zeitlich, in Bezug auf den Personenkreis). Ein Zwang zu Klarnamen zur Abtretung sämtlicher Urheberrechte ist aus Sicht des Präsidiumsarbeitskreises inakzeptabel.

III. Nutzung von Social Media

Die GI unterstützt den Einsatz von Informatiksystemen zur Verbesserung der lokalen und globalen Lebensbedingungen. Informatikerinnen und Informatiker tragen Verantwortung für die sozialen und gesellschaftlichen Auswirkungen ihrer Arbeit; sie sollen durch ihren Einfluss auf die Nutzung, Vermarktung und Weiterentwicklung von Informatiksystemen zu ihrer sozial verträglichen Verwendung beitragen.

Unter Beachtung der relevanten Bewertungskriterien und der Ethischen Leitlinien der GI ermutigt der Präsidiumsarbeitskreis die Mitglieder der GI zur Nutzung von Social Media insbesondere zur Förderung von interdisziplinären Diskursen zu ethischen und sozialen Problemen der Informatik. Dies kann auch Diskurse um Social Media selbst umfassen. Der Präsidiumsarbeitskreis ermutigt die Mitglieder der GI in Situationen, in denen die Nutzungsbedingungen von Social Media oder die Verhaltensweisen von Anbietern in Konflikt mit der Verantwortung gegenüber anderweitig Betroffenen stehen, mit Zivilcourage zu handeln.

Der Präsidiumsarbeitskreis übernimmt Vermittlungsfunktionen, wenn Beteiligte in Konfliktsituationen diesen Wunsch an sie herantragen. Unabhängig davon empfiehlt der Präsidiumsarbeitskreis die Beachtung folgender Regelungen bei der Nutzung von Social Media:

A. Nur seriöse Beiträge mit Vereinsbezug einstellen

Jeder Beitrag in einem sozialen Netzwerk mit Bezug zur GI wird von zahlreichen Nutzern in gewisser Weise als vereinsbezogene Äußerung angesehen. Daher sind Personen, die Beiträge mit Bezug zur GI in ein soziales Netzwerk einstellen, gut beraten, bei der Darstellung von solchen Beiträgen größten Wert auf Seriosität zu legen.

Zudem ist darauf zu achten, welcher Nutzerkreis in dem sozialen Netzwerk angesprochen wird. Bei Beiträgen mit Vereinsbezug ist folglich das passende Maß aus kompetenter Darstellung, zielorientierter Ansprache des vorgesehenen Adressatenkreises und des eigenen Profils (ggf. unter Einbeziehung der Unternehmens- bzw. Behördenkultur, bei der die einstellende Person beschäftigt ist) zu finden. Eingestellte Beiträge mit Bezug zur GI sind insoweit verständlich und nachvollziehbar abzufassen.

B. Bei eingestellten Beiträgen stets die Netiquette beachten

Einträge in soziale Netzwerke mit Bezug zur GI müssen authentisch sein.

Verunglimpfungen und rechtlich sanktionierbare Aktivitäten sind zu unterlassen; private Meinungsäußerungen auch als solche zu kennzeichnen. Die Meinungen anderer sind zu akzeptieren. Die Meinungsvielfalt innerhalb der GI ist ein hohes Gut. Mit etwaigen Fehlern, die im Kontext des sozialen Netzwerks versehentlich unterlaufen sind, ist offen umzugehen.

Bei Beiträgen mit Bezug zur GI ist auf Besonnenheit Wert zu legen. Eingestellte Beiträge mit Bezug zur GI dürfen insoweit nicht vereinsschädigend wirken. Soweit Kritik geäußert wird, hat dieses sachlich zu erfolgen und/oder unter ausdrücklicher Kennzeichnung der geäußerten Position als eigene Meinung.

C. Keine Verletzung von Rechten Anderer

Bei dem Upload von Dateien in soziale Netzwerke ist zuvor sicherzustellen, dass diese keine Metadaten (wie z.B. Geoinformationen) enthalten. Zudem ist zu berücksichtigen, dass bei Einstellung von Beiträgen in soziale Netzwerke meist aufgrund der dort geltenden Nutzungsbedingungen der Betreiber der Plattform Nutzungsrechte an eingestellten Texten, Bildern oder sonstigen Daten erhält.

Urheberrechte, Datenschutz und Geschäftsgeheimnisse sind daher bei allen Einträgen sorgfältig einzuhalten und Beiträge mit Bezug zur GI vorzugsweise nur in soziale Netzwerke einzustellen, deren Nutzungsbedingungen nicht einem häufigen Wandel unterliegen. Insbesondere sind bei der Verwendung eines Accounts in einem sozialen Netzwerk die Folgen zu beachten, die daraus resultieren können, wenn das eigene Profil bzw. ein spezifischer Beitrag gelöscht werden soll.

Soweit das soziale Netzwerk Wahlmöglichkeiten bei der Einstellung bietet, ist daher die Einstellung zu wählen, die für einen angemessenen Zugriffsschutz auf eingestellte Daten im Internet sorgt. Soziale Netzwerke, deren Einstellbarkeit für die Nutzer transparent und gut nachvollziehbar sind und zugleich nutzerfreundliche Datenschutz- und Nutzungsbedingungen aufweisen, sind daher für Darstellungen über Aktivitäten der GI besonders gut geeignet.

D. Mögliche Datenverwendungen durch Dritte berücksichtigen

Sobald Text- oder Bilddaten ohne spezifischen Zugriffsschutz in einem sozialen Netzwerk (und damit i.d.R. frei zugänglich im Internet) abgelegt werden, können diese Daten weltweit unbeschränkt (automatisiert) ausgewertet und auch für zielgerichtete Social-Engineering-Angriffe verwendet werden.

Da zudem einmal eingestellte Daten u.U. nur schwer oder gar nicht gelöscht werden können, verbleiben diese ggf. dauerhaft im Internet. Dies gilt im Besonderen für Daten, die ein Dritter über Andere eingestellt und evtl. sogar mit einer entsprechenden Kennzeichnung oder Geo-Tag versehen hat.

Aus diesen Gründen sind Daten mit Bezug zur GI, die dazu geeignet sind, einzelne Personen (aufgrund des abgebildeten Gesichts, aber auch aus sonstigen speziellen Merkmalen, Beschreibungen oder Angaben) identifizieren zu können, entweder nur mit deren wirksameren Zustimmung oder nur über Funktionsträger als Träger relativer Zeitgeschichte in soziale Netzwerke einzustellen.

E. Keine Fixierung auf ein einzelnes soziales Netzwerk

Sofern ein soziales Netzwerk zur Darstellung der GI verwendet wird, das nicht von der GI selbst betrieben wird, können alle eingestellten Beiträge mit Bezug zur GI nur freiwilligen Charakter haben. Das gilt insbesondere für Information über Aktivitäten der GI, die daher Mitglieder der GI auch auf mindestens einem weiteren Kommunikationsweg erreichen müssen. Kein soziales Netzwerk darf in diesem Sinne Exklusivrechte über Veröffentlichungen mit Vereinsbezug besitzen.

Bei Einstellungen von Beiträgen in sozialen Netzwerken ist daher darauf zu achten, dass diese vereinsbezogenen Angaben auch an anderer Stelle in geeigneter Form veröffentlicht bzw. den Mitgliedern zugestellt werden. Die zeitnahe Zusendung entsprechender Daten an die Geschäftsstelle der GI wird daher erwartet.

IV. Entwicklung von Social Media

Der Präsidiumsarbeitskreis empfindet eine besondere Verantwortung, die an der Entwicklung und dem Betrieb von Social Media beteiligten Personen auf die Bedeutung von „Data Protection by Design“ bzw. „Data Protection by Default“ hinzuweisen, die als relevante Punkte in die EU Datenschutzgrundverordnung aufgenommen wurden. Die grundlegenden Prinzipien wurden von Ann Cavoukian bereits in den 90er Jahre unter der Bezeichnung „Privacy by Design“ aufgestellt:

A. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe

„Data Protection by Design“ ist von proaktiven statt reaktiven Maßnahmen geprägt. Er sieht in die Privatsphäre vordringende Ereignisse voraus und verhindert sie, bevor sie geschehen können. Dieser Ansatz kommt zum Einsatz, bevor die Risiken für den Datenschutz aufgetreten sind. Es bietet keine Abhilfe im Falle von datenschutzrechtlichen Verletzungen, wenn sie erst einmal eingetreten sind – es verhindert vielmehr deren Auftreten. Kurz gesagt, „Data Protection by Design“ verhindert bereits im Vorfeld, dass Fakten geschaffen werden.

B. Datenschutz als Standardeinstellung

Standardeinstellungen sind entscheidend: „Data Protection by Design“ soll den größtmöglichen Schutz der Privatsphäre bringen, indem sichergestellt wird, dass personenbezogene Daten automatisch in jedem IT-System und bei allen Geschäftspraktiken geschützt werden. Wenn eine Person nichts unternimmt, bleibt der Schutz ihrer Privatsphäre immer noch intakt. Einzelpersonen sind nicht gefordert, selbst etwas für den Schutz ihrer Privatsphäre zu unternehmen – der Schutz ist als Standardeinstellung bereits systemimmanent.

C. Der Datenschutz ist in das Design eingebettet

„Data Protection by Design“ ist in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet. Es wird nicht nach einem Vorfall als Add-on eingebaut. Das Ergebnis ist,

dass der Datenschutz eine wesentliche Komponente der Kernfunktionalität wird. Datenschutz muss ein wesentlicher Bestandteil des Systems ohne Abstriche bei der Funktionalität sein.

D. Volle Funktionalität – eine Positivsumme, keine Nullsumme

„Data Protection by Design“ will allen berechtigten Interessen und Zielen entgegenkommen, und zwar durch eine Positivsumme, die ein zufriedenstellendes Ergebnis für beide Seiten erzielt, und nicht durch einen veralteten Nullsummenansatz, bei dem schließlich unnötige Kompromisse erforderlich werden. Durch diesen Ansatz wird die Vortäuschung falscher Dichotomien vermieden. „Data Protection by Design“ zeigt, dass es möglich ist, scheinbar konkurrierende Ziele zugleich zu erreichen.

E. Durchgängige Sicherheit - Schutz während des gesamten Lebenszyklus

Nachdem „Data Protection by Design“ vor der Ersterfassung der Information in das System „eingebettet“ wurde, erstreckt sich dessen Wirkung auf den gesamten Lebenszyklus der Daten - starke Sicherheitsmaßnahmen sind für den Datenschutz unerlässlich, und zwar von Anfang bis Ende. Dadurch wird erreicht, dass alle Daten sicher gespeichert und am Ende des Prozesses unwiderruflich vernichtet werden. So sorgt „Data Protection by Design“ durchgängig für eine sichere Datenverarbeitung.

F. Sichtbarkeit und Transparenz – Für Offenheit sorgen

„Data Protection by Design“ will allen Beteiligten die Sicherheit geben, dass das System unabhängig von Geschäftspraktiken oder Technologien wirklich die angekündigten Maßnahmen und Ziele verfolgt und sich einer unabhängigen Prüfung unterwirft. Seine einzelnen Komponenten und Verfahren bleiben sichtbar und transparent, und zwar gleichermaßen für Nutzer und Anbieter.

G. Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen

„Data Protection by Design“ erfordert vor allem von den Architekten und Betreibern (von IT-Systemen), dass für sie die Interessen der Einzelpersonen an erster Stelle stehen. Sie bieten Maßnahmen wie strenge datenschutzfreundliche Voreinstellungen und angemessene Benachrichtigungen an, eröffnen benutzerfreundliche Optionen und sorgen für eine nutzerzentrierte Gestaltung.

Kontakt:
Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Tel.: +49 (0)228/302-145 / Fax: +49 (0)228/302-167
E-Mail: gs@gi.de / WWW: http://www.gi.de

Präsidiumsarbeitskreis:
https://www.gi.de/themen/datenschutz.html