digitalcourage e.V. | Marktstraße 18 | D-33602 Bielefeld

Kommentar von digitalcourage zur EU-Datenschutz-Grundverordnung

Ihr Zeichen / Your Ref.
Unser Zeichen / Our Ref.
☎ 0521-1639.1639
Datum / Date
Thema / Subject

Anschrift / Address
digitalcourage e.V.
c/o Art d'Ameublement
Marktstraße 18
D-33602 Bielefeld

Telefon / Phone
Tel +49-521-1639.1639
Fax +49-521-61172

eMail / Web
mail@digitalcourage.de
www.digitalcourage.de
www.bigbrotherawards.de

ÖPNV / Public Transport
Stadtbahn ab Hauptbahnhof
alle Linien Haltestelle Rathaus

Konto / Bank Account
Shop-Konto 21 34 187
IBAN DE27 4805 0161 0002 1341 87
Spenden-Konto 21 38 113
IBAN DE46 4805 0161 0002 1381 13
Geschäfts-Konto 21 29 799
IBAN DE66 4805 0161 0002 1297 99
Sparkasse Bielefeld
(BLZ 480 501 61)
BIC: SPBIDE3BXXX

Eingetragen beim
Amtsgericht Bielefeld
VR 2479

Steuernummer / Tax
DE 187386083

digitalcourage ist vom
Finanzamt Bielefeld
als gemeinnützig
anerkannt.

Zusammenfassung:
Digitalcourage, als einer der Vorreiter des Datenschutzes und der Bürgerrechte im digitalen Zeitalter, begrüßt das Vorhaben der EU Kommission, den Datenschutz in den Mitgliedsländern zu harmonisieren und ein hohes Datenschutzniveau zu garantieren.

Eine Anpassung des Datenschutzes an die neuen Herausforderungen der digital vernetzten Welt ist unser Kernanliegen. Digitalcourage hat seit über 25 Jahren Expertise gesammelt. Diese stellt er im Rahmen seiner Möglichkeiten gerne der EU zur Verfügung.

Die Datenschutz-Grundverordnung der EU ist zu begrüßen. Sie muss die Informationelle Selbstbestimmung der Bürgerinnen und Bürger in den Mittelpunkt stellen. Sie darf unter keinen Umständen hinter das beste Datenschutzniveau eines der Mitgliedsländer der EU zurückfallen. Das Datenschutzniveau muss angehoben. Besonders die umfangreiche und angesehene deutsche Rechtsprechung und die Grundrechte auf Informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (das so genannte Computer-Grundrecht) dürfen in keiner Weise geschwächt werden.

Digital vernetzte Kommunikation erfordert im besonderen Maße die Durchsetzung der Rechte von EU-Bürgerinnen und Bürgern gegenüber Unternehmen und Datenverarbeitern innerhalb und außerhalb der EU. Das muss ein Kerngedanke der Datenschutz-Grundverordnung sein und gestärkt werden.

Lobenswertes:

Digitalcourage begrüßt die Einführung des „privacy by design“-Konzepts. Damit werden die Daten der Nutzerinnen und Nutzer nicht mehr automatisch freigegeben. Userinnen und User behalten damit die Kontrolle über ihre Daten. Die Daten werden erst freigegeben, wenn die Nutzerinnen und Nutzer das erlauben. In diesem Zusammenhang ist das Einwilligungs-Prinzip zu begrüßen, das die explizite Zustimmung der Betroffenen voraussetzt. Die Zustimmung muss mit einem Verfallsdatum versehen werden. Damit muss sie nach angemessener Frist neu eingeholt werden. Andernfalls müssen die erhobenen Daten automatisch gelöscht werden.

Kommentar zur EU-Datenschutz-Grundverordnung

Kritik:
Digitalcourage kritisiert die Verwässerung des aktuellen Entwurfs bei der Einwilligung zum Direktmarketing. Diese ist nun nicht mehr vorgesehen. Digitalcourage fordert diese Einwilligung weder aufzunehmen und Direktmarketing nur nach ausdrücklicher Einwilligung zu erlauben.

Digitalcourage fordert unabhängige Kontrollen. Damit diese wirksam sind, müssen die Datenschutzbehörden der EU und der Nationalstaaten mit ausreichend Mitteln ausgestattet sein. Es muss sichergestellt sein, dass Sanktionen und Strafen eine abschreckende Wirkung haben.

Digitalcourage ist seit 1987 eine der führenden Datenschutz- und Bürgerrechtsorganisationen in Deutschland und hieß früher FoeBuD. Seit 2000 richtet er die deutschen BigBrotherAwards aus. Er hat erfolgreich gegen die Vorratsdatenspeicherung und gegen ELENA beim Bundesverfassungsgericht geklagt. Das Thema RFID hat der FoeBuD in Europa und in Deutschland auf die Agenda gebracht.

Stellungnahme zu einzelnen Artikeln:

Digitalcourage begrüßt Artikel 7 („Einwilligung“) und fordert eine einfache und zumutbare Lesbarkeit der Datenschutzbestimmungen.
Verbraucherinnen und Verbraucher können nur in etwas einwilligen, das sie gelesen und verstanden haben. Datenschutzbestimmungen müssen deshalb in einfacher Sprache geschrieben und in zumutbarer Zeit lesbar sein. Die Folgen der Einwilligung müssen deutlich aus den Datenschutzbestimmungen hervorgehen.
Wir fordern Logos, die die Folgen von Datenschutzbestimmungen verständlich darstellen. Wir fordern auch eine maschinenlesbare Beschreibung des Inhalts von Datenschutzbestimmungen. Auf diese Weise kann automatisiert dargestellt werden, welche Folgen eine Einwilligung in die Datenschutzbestimmung hat. Denkbar sind Browser-Plugins, die auf einen Blick zeigen, ob die Datenschutzbestimmungen den Wünschen der Nutzenden entsprechen oder nicht. Hierin sieht digitalcourage einen sehr innovativen Ansatz.
Eine Einwilligung zur Datenverarbeitung muss mit einem Ablaufdatum versehen sein. Eine einmal gegebene Einwilligungen bleibt damit nicht unbestimmt gültig, wenn sie vergessen wurde.
Wir fordern ein Kopplungsverbot, damit die Einwilligung in die Datenverarbeitung freiwillig erfolgt und nicht daran geknüpft wird, einen bestimmten Dienst nutzen zu können.

Digitalcourage begrüßt Artikel 11: („Transparenz“).
Zu transparenten Informationen für die Verbraucherinnen und Verbraucher

gehören die Folgen einer Einwilligung in die Datenverarbeitung. Damit der Anspruch an Transparenz verwirklicht wird, müssen die Folgen der Datenverarbeitung in klarer Sprache und zumutbarer Länge dargestellt werden.

Digitalcourage fordert, Artikel 6, Abs. 1, Satz f zu streichen.
Dieser Satz bestimmt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, wenn sie der „Wahrung berechtigter Interessen" dient. Das ist eine carte blanche, da „berechtigte Interessen" ein unbestimmter Rechtsbegriff ist. Die anderen in Abs. 1 geregelten Erlaubnistatbestände für eine Datenverabeitung reichen völlig aus.

Digitalcourage fordert die Ausweitung des Auskunftsrecht in Artikel 15.
Das Auskunftsrecht für betroffene Personen muss erweitert werden um Auskunft über die logische Art der Datenverarbeitung. Nur wenn Verbraucherinnen und Verbraucher über die Art und Weise, wie Daten über sie verarbeitet werden, informiert sind, können sie ihre Rechte wahrnehmen. Deshalb müssen die Algorithmen, mit denen Daten verarbeitet werden, offen gelegt werden.
Auch Datenschutz- und Verbraucherschutzverbände müssen ein generelles Auskunftsrecht darüber erhalten, wie Daten gespeichert werden.

Digitalcourage fordert eine Ausweitung des „Rechts auf Vergessenwerden" in Artikel 17.
Daten müssen nicht nur gelöscht werden, wenn sie öffentlich gemacht wurden. Es müssen auch alle Schritte unternommen werden, die Daten zu löschen, wenn sie an Dritte weitergegeben wurden, die die ihrerseits veröffentlicht haben.

Digitalcourage begrüßt das „Recht auf Datenübertragbarkeit" und fordert Interoperabilität (Artikel 18).
Dabei muss es unerheblich sein, in welchem Format Anbieter die Daten intern speichern. Die Daten müssen in jedem Fall in einem „verwendbaren strukturierten gängigen elektronischen Format" zugänglich gemacht werden.
Soziale Netzwerke haben großartigen kommunikativen Wandel angestoßen, bei dem derzeit kein Wettbewerb herrscht. So wie es möglich ist, den E-Mail-Anbieter zu wechseln oder von einem Anbieter eine E-Mail zu einem anderen Anbieter zu schreiben, so müssen Soziale Netzwerke untereinander kompatibel sein. Offener, fairer Wettbewerb ist eine der Grundsäulen der EU, der nur auf diese Weise verwirklicht werden kann.
Dafür fordert digitalcourage offene Schnittstellen und offene Standards.

Digitalcourage kritisiert Artikel 19 („Widerspruch").
Dieser Artikel ist im Vergleich zum vorhergehenden Entwurf von einem opt-in zu einer Widerspruchslösung verwässert worden. Digitalcourage fordert eine opt-in

Lösung. Diese ist im Sinne der Verbraucherinnen und Verbraucher. Andernfalls wird Arbeit auf die Verbraucherinnen und Verbraucher abgewälzt, die selbst tätig werden müssen, wenn sie vom Direktmarketing verschont bleiben wollen.

Digitalcourage kritisiert Artikel 20 („Profiling“).
Digitalcourage fordert, dass sensible Daten, etwa Gesundheitsdaten, zu keiner Zeit zum Profiling verwendet werden dürfen. Profiling von Kindern muss verboten sein.
Profile sind auch dann personenbezogen, wenn die Personendaten nicht bekannt sind, es sich aber um eindeutige Profile, etwa Browser oder Kreditkartenprofile, handelt. Sie sind eindeutig wiedererkennbar und deshalb personenbezogen. Auch anonymes oder pseudonymes Profiling muss eine Einwilligung erfordern.

Digitalcourage kritisiert Artikel 42 („Datenübermittlung an Drittstaaten“).
Digitalcouarge fordert, dass Auskünfte an Behörden von Drittstaaten nur rechtmäßig sind, wenn der Auskunftsgrund auch innerhalb der EU eine Rechtsgrundlage hat. Selbstverpflichtungen der anfragenden Unternehmen (wie zum Beispiel Safe Harbor) oder staatlichen Stellen aus Drittländern sind nicht geeignet, diese gesetzlichen Grundlagen zu ersetzen.