



Sehr geehrte Abgeordnete des Europäischen Parlaments,

die unterzeichnenden Organisationen fordern das Europäische Parlament nachdrücklich auf, ein hohes Niveau an Datenschutz und Vertraulichkeit in der geplanten ePrivacy-Verordnung zu gewährleisten und die Schwächen der aktuellen Position des Rates während der Trilogverhandlungen zu beheben.

Vor vier Jahren schlug die Europäische Kommission die Datenschutzverordnung für elektronische Kommunikation (ePrivacy Regulation/-Verordnung) vor, um die von der DSGVO begonnene Modernisierung des EU-Datenschutzrahmens abzuschließen. **Um die Bedenken hinsichtlich der Verwendung von Cookies und anderen Tracking-Technologien auszuräumen**, hat das Europäische Parlament folgende Bestimmungen beschlossen:

- **Der Schutz von Internetnutzern vor Tracking und Überwachung, sei es durch Cookies oder andere technische Mittel.** Das Sammeln oder Speichern von Daten auf dem Gerät eines Benutzers ist nur mit Zustimmung des Benutzers gestattet, es sei denn, dies ist für den Dienst technisch erforderlich (Artikel 8).
- **Das Verbot von Tracking- oder Cookie-Walls**, die Benutzer dazu zwingen sollen, der Verarbeitung oder Speicherung zusätzlicher Daten im Austausch für den Zugriff zuzustimmen (Artikel 8).
- **Die Entlastung der Internetnutzer durch technische Datenschutzeinstellungen**, mit denen sie die Auswahl von Einwilligungen automatisieren und rechtsverbindliche Signale von Hardware oder Software verwenden können, die an die Webseite übermittelt werden (Artikel 9 und 10). Artikel 19 legte ein Verfahren für die Spezifikation solcher Signale durch die Europäische Datenschutzbehörde fest.

Diese Schutzmaßnahmen wurden vom Rat in seinem Verhandlungsmandat beseitigt oder geschwächt.

Artikel 8 Abs. 1 Buchstaben a, c und d des Rates schaffen Unklarheiten über die für einen Dienst „technisch erforderlichen“ Daten und öffnen die Tür für das Tracken von Nutzern. Darüber hinaus wurde das Verbot von „Tracking-Walls“ in einen Erwägungsgrund verschoben und unter unklare Vorbehalte gestellt.

Der Rat hat auch die Artikel 9 und 10 gestrichen und sich von den technischen Lösungen und den Forderungen von Zustimmungslösungen bei Datenerfassung abgewandt. Infolgedessen müssen sich Benutzer den anhaltenden Belästigungen durch Zustimmungsbanner stellen, die versuchen, sie mit „Dark Pattern“ (unethischen Webseitenmustern) zu manipulieren. Anstelle solcher Anfragen könnten rechtsverbindliche Signale treten, die vom Benutzer konfiguriert wurden. Diese Lösung bleibt jedoch nun Wunschdenken und wird in einen Erwägungsgrund verwiesen. In Bezug auf das „Privacy by Design“ (datenschutzfreundliche Gestaltung) und „Privacy by Default“ (Datenschutz durch Voreinstellung) **haben sich die meisten Browser dem Schutz ihrer Benutzer verschrieben. Diese Entwicklung wird in der Verordnung nicht aufgegriffen, sie sollte deutlich mehr berücksichtigt und ausgebaut werden.**

Seit das Parlament im Oktober 2017 seinen Standpunkt festgelegt hat, wurde das Vertrauen der Öffentlichkeit in die Internetdatenverarbeitung durch den Cambridge Analytica Skandal beeinträchtigt. Von der ePrivacy-Verordnung muss die klare Botschaft ausgehen, dass die Zukunft eher Geschäftsmodellen gehört, die Grundrechte und Innovation vereinen, als solchen, die gezielt und massenhaft persönliche Daten abschöpfen.

**Der Standpunkt des Rates legitimiert stattdessen Missbräuche und Verstöße gegen das Datenschutzrecht und es gelingt ihm nicht auf das Vertrauensdefizit einzugehen.** In einer Eurobarometer-Umfrage von 2016 gaben „mehr als sieben von zehn NutzerInnen von Internet- und Online-Plattformen an, dass sie über die im Internet über sie gesammelten Daten besorgt sind“. Im Jahr 2020 haben Studien ergeben, dass ein Drittel der VerbraucherInnen auf diese Bedenken reagiert und mit mindestens einem Unternehmen den Kontakt aus Datenschutzgründen beendet hat. Dieselbe Studie ergab, dass weitere 87% der Befragten besorgt waren, dass ihre Daten durch die Tools, die sie aufgrund der COVID-19-Pandemie für die Arbeit im Homeoffice benötigen, nicht ausreichend geschützt sind.

Wir fordern das Europäische Parlament dringend auf, seine Position zu bekräftigen und sicherzustellen, dass die ePrivacy-Verordnung ihre Ziele erreicht. Personenbezogene Daten im Bereich der elektronischen Kommunikation sind äußerst sensibel, da sie intime Aspekte des Privatlebens von Einzelpersonen offenlegen, insbesondere weil derzeit aufgrund der Pandemie alltägliche Aktivitäten und Kommunikationen überwiegend online stattfinden. **Der durch die DSGVO gewährte Schutz sollte deshalb dahingehend ergänzt werden, dass Lücken geschlossen und Grauzonen aufgehellt werden, die von der Trackingbranche in großem Umfang missbraucht wurden, sowie indem zusätzliche, stärkere Garantien zur Reglementierung der Verarbeitung personenbezogener Daten in diesem Bereich geschaffen werden.**

Wir fordern das Europäische Parlament auf, die Stellungnahmen des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten umfassend zu berücksichtigen und Vorschläge oder Kompromisse abzulehnen, die das Schutzniveau der DSGVO und der aktuellen Datenschutzrichtlinie für elektronische Kommunikation verringern würden.

Mit freundlichen Grüßen

- Access Now, International
- Amnesty International
- BEUC, The European Consumer Organisation
- Bits of Freedom, The Netherlands
- Centre for Peace Studies, Croatia
- Civil Liberties Union for Europe (Liberties), International
- Civil Rights Defenders, Sweden
- Coalition for Civil Liberties and Rights, Italy
- Communia, International
- Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany
- Digitalcourage, Germany
- Electronic Frontier Foundation, International
- Free Knowledge Advocacy Group EU, International
- Homo Digitalis, Greece
- Human Rights Monitoring Institute, Lithuania
- Hungarian Civil Liberties Union, Hungary
- Institute of Information Cyprus, Cyprus
- IT-Pol Denmark, Denmark
- Liga lidských práv | League of Human Rights, Czech Republic
- Ligue des Droits Humains, Belgium
- Netzwerk Datenschutzexpertise, Germany
- Open Rights Group, United Kingdom
- Panoptykon Foundation, Poland
- Platform Bescherming Burgerrechten, The Netherlands
- Privacy First, The Netherlands
- Privacy International, International
- Ranking Digital Rights, USA
- The Irish Council for Civil Liberties, Ireland
- The Privacy Collective, International
- Xnet, Spain