S&D WIR IN EUROPA

Die SPD-Abgeordneten – Fraktion der Sozialdemokraten im Europäischen Parlament

STANDPUNKT
DATENSCHUTZ

DATENSCHUTZ-STANDARDS FÜR GANZ EUROPA DURCHGESETZT – EINSATZ FÜR MEHR ONLINE-PRIVATSPHÄRE

Datenschutz ist ein europäisches Grundrecht. Ob beim Versand einer E-Mail, beim Arztbesuch oder im Bewerbungsverfahren – wir haben das Recht, dass unsere persönlichen Daten nicht missbraucht werden oder den Falschen in die Hände fallen. In einer zunehmend digitalisierten Welt drohen jedoch Daten, die teils persönlichste Details aus unserem Leben offenbaren, zur bloßen Ware für Konzerne zu werden. Wir Sozialdemokratinnen und Sozialdemokraten stehen für eine gerechte Gestaltung der Digitalisierung, in der die Menschen darauf vertrauen können, dass der Staat den Schutz ihres digitalen Lebens garantiert. Das geht nur mit einem EU-weit möglichst einheitlichem Datenschutz. Seit Mai 2018 greift EU-weit die Datenschutzgrundverordnung. Sie ist ein Meilenstein für das EU-Grundrecht auf Datenschutz und setzt weltweit Standards für einen verbraucherfokussierten Datenschutz.

DATENSCHUTZ

Die SPD-Abgeordneten – Fraktion der
Sozialdemokraten im Europäischen Parlament

Das zuvor geltende EU-Datenschutzrecht stammte noch aus dem Jahr 1995 – als das Internet noch jung war und Smartphones von einem anderen Planeten schienen.

Die SPD-Gruppe hat diese Reform stets unterstützt. Aber insbesondere von konservativer Seite gab es viele Torpedierungsversuche mit dem Ziel, multinationalen Konzernen mehr Rechte einzuräumen als Bürgerinnen und Bürgern. Auch gegen die Richtlinie zur Stärkung des Grundrechts auf Datenschutz in der Strafverfolgung gab es lange großen Widerstand aus der konservativen Fraktion, zu der auch die deutsche CDU/CSU-Gruppe gehört.
Nun liegt es an den Aufsichtsbehörden, die neuen Möglichkeiten zur Sanktionierung von Datenschutzverstößen, insbesondere der großen Internetgiganten, vollumfänglich auszuschöpfen. Wir Sozialdemokratinnen und Sozialdemokraten pochen deswegen auf eine angemessene personelle und finanzielle Ausstattung der Datenschutzbehörden durch die EU-Mitgliedstaaten. Nur so können wir sicherstellen, dass jene Behörden, welche die Anwendung der neuen europäischen Datenschutzregeln sicherstellen sollen, auch tatsächlich gut arbeiten können.

Die Datenschutzgrundverordnung war ein wichtiger erster Schritt, wir Sozialdemokratinnen und Sozialdemokraten wollen jedoch mehr: Neben dem reinen Datenschutz müssen wir auch die Vertraulichkeit elektronischer Kommunikation als Ganzes besser schützen – also das Briefgeheimnis ins 21. Jahrhundert transportieren. Wer etwa im Internet unterwegs ist, soll besser vor unerwünschter Werbung und Nachspionieren („tracking“) geschützt werden.
Ob geschäftliche E-Mail oder Katzenvideo – was wir wann, wo und an wen schicken, muss vertraulich sein. Deshalb wollen wir in der Legislaturperiode 2019 bis 2024 den konservativen Widerstand gegen die geplante ePrivacy-Verordnung zum Schutz unserer Online-Kommunikation brechen.

WESENTLICHE ERFOLGE BEI DER DATENSCHUTZ-GRUND-VERORDNUNG:

EINHEITLICHE REGELN FÜR DIE GESAMTE EU:

Bisher galten in der EU 28 verschiedene Datenschutzstandards. Die Datenschutz-Verordnung schafft ein einheitliches Set von Regeln. Das hat Vorteile für Unternehmen, die in mehr als einem Mitgliedstaat tätig sind. Aber es hat auch Vorteile für Unternehmen in Deutschland, die weniger Wettbewerbsnachteile dadurch haben, dass anderswo in Europa die Datenschutzregeln laxer sind. Bisherige Wettbewerbsnachteile gegenüber außereuropäischen Anbietern werden zudem dadurch abgemildert, dass sich alle Anbieter von Produkten und Dienstleistungen auf dem EU-Markt an die Datenschutz-Verordnung halten müssen. Die Datenschutz-Verordnung erkennt gleichzeitig explizit die besondere Situation von kleinen und mittleren Unternehmen an und hält die Aufsichtsbehörden an, bei der Anwendung der neuen Datenschutzregeln ihre besonderen Bedürfnisse zu berücksichtigen.

STÄRKUNG DER RECHTE DER NUTZERINNEN UND NUTZER:

Transparenz, „Recht auf Vergessen", Datenportabilität, Schutz vor Profiling: Eine wesentliche Voraussetzung für die Wahrnehmung eigener Rechte ist Transparenz über die bestehenden Prozesse zur Datenverarbeitung. Die Datenschutz-Verordnung verpflichtet Datenverarbeiter, Betroffene umfassend zu informieren, etwa über den Zweck der Datenverarbeitung, die Rechtsgrundlage für die Verarbeitung oder die Speicherdauer. Zudem wird ein „Recht auf Vergessenwerden" verankert: Verbraucherinnen und Verbraucher können etwa von einem Unternehmen verlangen, dass über sie gespeicherte Daten gelöscht werden. Zum Beispiel, weil die Daten für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind oder weil der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat. Wenn die betroffenen Daten öffentlich gemacht wurden, müssen auch Dritte, die auf die Veröffentlichung hinweisen, über den Wunsch der Verbraucherin oder des Verbrauchers zur Löschung der Daten informiert werden. Ausnahmen gelten etwa für Personen des öffentlichen Lebens. Neu ist zudem das Recht auf Datenportabilität, das den „Umzug" der eigenen Daten etwa von einem Dienst zum anderen erleichtern soll. Die Datenschutz-Verordnung schützt den Einzelnen zudem besser vor den negativen Konsequenzen von Profiling.

STRENGE ANFORDERUNG AN DIE EINWILLIGUNG:

Es gibt verschiedene rechtmäßige Möglichkeiten, um Daten zu erheben, verarbeiten und zu speichern. Eine Möglichkeit ist die Zustimmung durch die Nutzerin oder den Nutzer, welche durch die Datenschutz-Verordnung nun gestärkt wird. Sie legt strenge Regeln dafür fest, wann eine Einwilligung rechtens ist und wann nicht. Das soll den Nutzer davor schützen, dass Anbieter sich eine angebliche Zustimmung zu einer Datenverarbeitung im Kleingedruckten der AGB erschleichen. Eine rechtmäßige Einwilligung muss freiwillig und spezifisch, also für den bestimmten Fall abgegeben sein. Sie muss informiert sein, d.h., der Nutzer versteht, um was es geht, und sie muss unmissverständlich und widerrufbar sein. Eine Einwilligung, die unter Missachtung dieser Prinzipien erschlichen wird, ist ungültig.

Die SPD-Abgeordneten – Fraktion der
Sozialdemokraten im Europäischen Parlament

EINE ANSPRECHPARTNERIN ODER EINEN ANSPRECHPARTNER FÜR ALLE DATENSCHUTZBELANGE:

Egal, wo in der EU ein Datenmissbrauch passiert, Betroffene können sich an ihre heimische Datenschutzbehörde wenden. Wenn ich also eine Beschwerde gegen eine Firma einlegen möchte, die in Irland sitzt, muss ich mich als deutsche Bürgerin oder als deutscher Bürger nicht mehr mit einer fremden Sprache und einem fremden System herumschlagen: Es reicht, sich an die deutschen Behörden zu wenden. Für Unternehmen ist die Datenschutzbehörde des EU-Mitgliedstaates, in dem sie ihren Sitz haben, der zuständige Ansprechpartner.

DATENSCHUTZ DURCH SINNVOLLE GESTALTUNG DER TECHNIK:

Dienste sollen so datensparsam wie nur möglich konzipiert sein. Alle Voreinstellungen zum Beispiel in einer Software sollen die datenschutzfreundlichsten sein. Ein wesentliches Merkmal von Datenschutz durch Technik ist, dass tatsächlich nur die Daten verarbeitet werden, die für die Erbringung eines Dienstes benötigt werden.

STRENGE REGELN :

Strenge Regeln für Datentransfers in Drittstaaten/ Weiterentwicklung von weltweiten Datenschutzstandards: In einer globalisierten Welt machen personenbezogene Daten nicht vor den EU-Außengrenzen halt, sondern fließen auch in Länder mit anderen Datenschutzregeln. Das EU-Recht schreibt vor, dass bei Datentransfers in Drittstaaten ein angemessenes Datenschutzniveau sichergestellt sein muss. Die Schutzstandards im Drittland müssen dabei keine genaue Kopie der EU-Regeln sein. Aber der Europäische Gerichtshof hat in seinem Urteil zur Aufhebung der so genannten Safe Harbor Vereinbarung zur Weitergabe von Daten in die USA klar gesagt, dass die Schutzstandards im Drittland „der Sache nach gleichwertig“ sein müssen. Das ist wichtig, weil wir so sicherstellen, dass unsere Daten nicht nur in Europa geschützt sind, sondern auch, wenn sie in die Welt verschickt werden. Damit trägt die Datenschutzverordnung auch zur Weiterentwicklung von Datenschutzstandards weltweit bei, da Länder, die mit uns Handel treiben wollen und auf Datentransfers angewiesen sind, Datenschutzstandards haben müssen, die mit unseren vergleichbar sind.

SANKTIONEN:

Bisher beliefen sich in Deutschland die Strafen für Datenschutzverstöße auf maximal 300.000 Euro. Über so einen Betrag können Facebook und Co. nur lachen. Wenn es günstiger ist, eine Strafe billigend in Kauf zu nehmen, als Grundrechte zu sichern, dann läuft etwas schief. Künftig können die Geldbußen bis zu 4 Prozent des weltweit erzielten Jahresumsatzes oder aber eine Summe von bis zu 20 Millionen Euro (welche immer höher ist) betragen. Damit soll erreicht werden, dass sich auch die großen Internetgiganten an europäisches Recht halten. Umgekehrt bedeutet es aber NICHT, dass jeder kleine Betrieb gleich den finanziellen Ruin fürchten muss. Bevor es überhaupt zur Verhängung einer Strafe kommt, ist zunächst mit einer Warnung und einem Maßnahmenvorschlag seitens der Aufsichtsbehörde zu rechnen, die die bestehenden Defizite beseitigen sollen. Geldstrafen und ihre Höhe sollen zudem immer mit Rücksicht auf die Art, Schwere und Dauer des Verstoßes verhängt werden.

Die SPD-Abgeordneten – Fraktion der
Sozialdemokraten im Europäischen Parlament

Stand Mai 2019

KONTAKT / HERAUSGEBER

Büro Berlin:
Europäisches Parlament
Fraktion der S&D
Deutsche Delegation
Deutscher Bundestag
Platz der Republik 1
11011 Berlin
Telefon: + 49 30 2277 1273
E-Mail: europabuero.spd@bundestag.de

Büro Brüssel:
Europäisches Parlament
Fraktion der S&D
Deutsche Delegation
Rue Wiertz
1047 Brüssel / Belgien
Telefon: + 32 2 284 3190
E-Mail: s-d.delegationDE@ep.europa.eu

Herausgeber: Jens Geier (V.i.S.d.P.)