Microsoft
Corporate Affairs Europe | Tel +32 (0) 2 704 39 10
Avenue de Nerviens 85 | B-1040 Brussels

Für weitere Informationen kontaktieren Sie bitte Jean Gonié, Director of Privacy EMEA Policy
oder Tanja Böhm, Manager Government Affairs, tanja.boehm@microsoft.com
oder Jörg-Alexander Albrecht, Manager Government Affairs, a-joalb@microsoft.com

Microsoft-Positionen zu grundlegenden Regelungen im vorliegenden Entwurf für die *Datenschutz-Grundverordnung*

Einwilligung

- Microsoft unterstützt eine informierte und sinnvolle Einwilligungsregelung ohne Erfordernis einer ausdrücklichen oder „positiven" Einwilligung und ohne zeitliche Beschränkung der Wirksamkeit der Einwilligung.
- Nach dem Verordnungsentwurf könnte die Notwendigkeit einer ausdrücklichen Einwilligung als Erfordernis verstanden werden, dass online-tätige Controller die Nutzer zur ausdrücklichen positiven Erlaubnis („opt in") der Nutzung ihrer Daten zwingen. Microsoft vertritt die Ansicht, dass dieser Ansatz eines allgemeingültigen „Universalkonzepts" zu eng ist. Derzeit gibt es eine ganze Reihe von Mechanismen, die den Nutzern, abhängig von den Umständen des Einzelfalles, effektiv die Kontrolle und Einwilligung zur Erhebung und Nutzung ihrer Daten ermöglichen, einschließlich von Op-out-Technologien, die einen stärkeren Schutz für den Datenschutz von Verbrauchern bieten als manche Opt-in-Mechanismen. Zum Beispiel trägt ein Opt-out-Mechanismus, der vollständige Informationen über die Art und Weise der Nutzung personenbezogener Daten bietet, dem Datenschutz in höherem Maße Rechnung als ein Opt-in-Mechanismus, der keine vollständigen Informationen enthält. Durch Bevorzugung eines Mechanismus gegenüber anderen verringert die Verordnung die Anreize zur Entwicklung verschiedener und möglichweise besserer Lösungen für den Datenschutz.
- Ebenso wichtig ist die Nachfrage von Verbrauchern nach Internetdienstleistungen, die schnell, einfach in der Anwendung und effizient sind. Wenn Nutzer in jede Nutzung ihrer Daten einwilligen müssen, wird die Verordnung möglicherweise verlangen, dass Internetnutzer unzählige Male per opt-in während einer einzigen Web-Sitzung oder einer mobilen Internetnutzung einwilligen müssen. Mühselige und statische Opt-in-Mechanismen können letztlich dazu führen, dass Nutzer routinemäßig auch in solchen Fällen einwilligen, in denen dem Schutz ihrer Privatsphäre besser mit einem Opt-out gedient wäre.
- Das Cloud-Computing, große Datenmengen und die starke Verbreitung von unterschiedlichen Geräten zur Datenverarbeitung eröffnen Gelegenheiten zur Zusammenfassung von Daten aus verschiedenen und zum Zeitpunkt der Datenerhebung nicht immer konkret vorhersehbaren Quellen und schaffen damit neue und nutzbringende Dienstleistungen. Ein Navigationssystem kann zum Beispiel Daten aus dem Fahrverhalten des Nutzers, Suchmuster, Verkehrsberichte und andere öffentliche Informationen zur Erstellung einer auf die Person abgestimmte Fahrtrichtung unter Berücksichtigung der Bedürfnisse und Vorlieben einer Person kombinieren und damit Zeitersparnis und verbesserte Produktivität erzielen. Aus einem vom Weltwirtschaftsforum in

Zusammenarbeit mit der Boston Consulting Group (BCG) erarbeiteten Bericht mit dem Titel „Unlocking the value of personal data“[1] geht ferner hervor, dass die Komplexität der Anwendungen, die transformative Kraft der verschiedenen Datennutzungen (in Bereichen wie Gesundheit, Infrastruktur, staatliche Dienstleistungen usw.) ein Überdenken der herkömmlichen Einstellungen zur Daten-Governance, insbesondere eine stärkere Berücksichtigung des Kontexts erfordern, um verschiedene Möglichkeiten der Datennutzung in unterschiedlichen Zusammenhängen zu eröffnen.

- **Die Einwilligung zur Verarbeitung personenbezogener Daten ist naturgemäß kontextuell.** Unternehmen, die ihre Datenverarbeitung von der Einwilligung des Betroffenen abhängig machen, *sollten* verpflichtet werden sicherzustellen, dass die Erklärung der Einwilligung nach entsprechender und sinnvoller Aufklärung erfolgt, was in der Verordnung auch so vorgesehen ist. Die Verordnung sollte Innovatoren jedoch die Verwendung verschiedener Mechanismen zur Einholung der Einwilligung ermöglichen, aus denen hervorgeht, wie und in welchem Kontext Einwilligungen eingeholt und Daten genutzt werden.

Berechtigtes Interesse

- Das berechtigte Interesse bildet eine wesentliche Grundlage für die Verarbeitung personenbezogener Daten und ist für eine breite Palette von Geschäftsaktivitäten und Verbraucherdienstleistungen sowie für eine große Anzahl von Verarbeitungstätigkeiten, die im besonderen Interesse bzw. zum besonderen Vorteil der betroffenen Personen selbst durchgeführt werden, von entscheidender Bedeutung, wie zum Beispiel die Erbringung von Dienstleistungen an die betroffenen Personen und deren Verbesserung. Ferner stellt das berechtigte Interesse eine wesentliche Rechtsgrundlage für die Entwicklung konkurrenzfähiger und innovativer Geschäftsmodelle für die europäische Informationsgesellschaft und für eine wissensgestützte Wirtschaft dar.
- Das berechtigte Interesse sollte eindeutig definiert werden, um eine zur Verbesserung des Datenschutz-Ökosystems beitragende Konsistenz zu gewährleisten. Die Definition des berechtigten Interesses sollte die Datenverarbeitung für Direktwerbung, die Sicherheits- und Leistungsüberwachung, die Beantwortung von Anfragen der Strafverfolgungs- und Vollzugsbehörden, den Schutz geistigen Eigentums, die Ermittlung und Bekämpfung von Betrug und anderen schädigenden Aktivitäten, die Durchsetzung von Rechtsansprüchen, das Recherchieren für historische, statistische oder wissenschaftliche Zwecke, die öffentliche Sicherheit, das öffentliche Gesundheitswesen, den sozialen Schutz und die Vertragserfüllung berücksichtigen.
- Die grundlegenden Rechte der betroffenen Person sollten ein entscheidendes Kriterium für die Entscheidung zur Verarbeitung der personenbezogenen Daten unter Gewährung von

[1] “Unlocking the value of personal data: From collection to usage”, World Economic Forum. Prepared in collaboration with BCG. February 2013. http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

Möglichkeiten für die betroffene Person zur Einlegung eines angemessenen Widerspruchs sein. Ferner sollte das Alter der betroffenen Person zwar nicht allein ausschlaggebend sein, jedoch als weiterer Faktor berücksichtigt werden, da betroffene Personen aller Altersgruppen von Betrug, kriminellen Handlungen und Sicherheitsverletzungen betroffen sein können.

Profiling

- Die Nutzung des Internets und die weite Verbreitung vernetzter Geräte erzeugen beispiellose Datenmengen, die gelegentlich zur Erstellung von Persönlichkeitsprofilen genutzt werden können. Das Profiling selbst ist ein rein technischer Prozess, der die Feststellung von Mustern aufgrund großer Datenmengen unterstützt und dabei die Erhebung und zielgerichtete Einordnung von Daten ermöglicht. Für sich genommen ist gegen das Profiling seinem Wesen nach nichts einzuwenden. In der Tat werden Profile häufig zur Erfüllung der Nachfragen von Verbrauchern nach Technologien und Dienstleistungen verwendet, die sich ihre Einstellungen, beispielsweise Muttersprache oder Heimatland, merken oder die den Bedürfnissen des Verbrauchers in anderer Hinsicht angepasst sind.
- Wie bei jedem geschäftlichen Prozess können automatische Profile natürlich auch für unerwünschte Zwecke, wie der Diskriminierung von Personen aufgrund ihrer Gesundheit, verwendet werden. Um zu gewährleisten, dass die Nutzerdaten nicht für Zwecke verwendet werden, die den Interessen von EU-Bürgern entgegenstehen, ist es durchaus sinnvoll, die Verwendung von Profilen für nachteilige Zwecke zu regulieren. Ein derartiges Regelwerk sollte jedoch nicht zu einer generellen Beschränkung der Erstellung von Profilen ungeachtet des Erstellungszwecks – einschließlich von nützlichen Zwecken als Reaktion auf berechtigte Forderungen von Verbrauchern – führen.
- **Einem starken Schutz der betroffenen Personen ist es dienlicher, wenn die Verordnung auf die Art der Profilverwendung, statt auf den für die Profilerstellung eingesetzten Mechanismus abstellt.** Die Verordnung sollte entsprechend geändert werden, um klarzustellen, dass Profile auch weiterhin für nützliche Zwecke, wie für die Bereitstellung von an die Nutzer angepassten Interneterfahrungen, die Ermittlung und Bekämpfung von Betrug und sonstigen kriminellen oder schädigenden Handlungen sowie für sonstige wichtige Zwecke, verwendet werden können. Zum Beispiel kann ein möglicher Kreditkartenbetrug von einer Bank auf der Grundlage des Profils des rechtmäßigen Inhabers der Kreditkarte durch Identifizierung „verdächtiger“ Transaktionen festgestellt und verhindert werden. Zu weit gefasste Profiling-Beschränkungen, wie Beschränkungen der einzelnen Bestandteile eines Profils, behindern Innovationen und sind mit zusätzlichen Risiken verbunden.
- Ferner unterstützt Microsoft Beschränkungen der Verwendung von Profilen in Fällen, in denen Profile nachteilige Rechtsfolgen für die betroffene Person haben können – beispielsweise die Analyse oder die Vorhersage der Arbeitsleistung der betroffenen Person,

der wirtschaftlichen Situation, von gesundheitlichen Entscheidungen, der Verlässlichkeit oder des Verhaltens – einschließlich der Möglichkeit der betroffenen Person, Widerspruch einzulegen, eine Erläuterung der Entscheidungsgründe zu verlangen und der Gelegenheit der betroffenen Person zur Einreichung einer Stellungnahme. Microsoft unterstützt außerdem Beschränkungen der Verwendung von Profilen für Zwecke, die dem Gemeinwohl und der Rechtsordnung entgegenstehen, wie zum Beispiel rechtswidrige Diskriminierung.

Das Recht auf Vergessenwerden (digitaler Radiergummi)

- Gemäß der Richtlinie 95/46 sind die für die Verarbeitung der Daten Verantwortlichen („Datencontroller“) verpflichtet, in bestimmten Fällen personenbezogene Daten auf Anweisung der betroffenen Person zu löschen. Die Verordnung baut auf diesem Grundsatz auf, indem sie Personen ein „Recht auf Vergessenwerden“ (digitaler Radiergummi) gewährt. Wie in der Verordnung vorgesehen, würde das Recht auf Vergessenwerden die Unternehmen nicht nur unter bestimmten Umständen zur Löschung von personenbezogenen Daten auf Verlangen einer betroffenen Person verpflichten, sondern das beteiligte Unternehmen müsste in Fällen einer erfolgten Veröffentlichung der Daten auch Auftragsverarbeiter der Daten über das Verlangen nach Löschung von Kopien der Daten oder von Links zu den Daten in Kenntnis setzen.
- **Die Struktur des Rechts auf Vergessenwerden trägt der Struktur des Internets jedoch nicht in vollem Umfang Rechnung.** Digitale Daten werden heute oft schnell über das gesamte Web auf Systemen und Servern weltweit mit oder ohne förmliche, technische oder vertragliche Beziehungen zwischen den verschieden Teilen des Online-Ökosystems kopiert. So verwenden zum Beispiel viele Suchmaschinen und Inhaltsaggregatoren öffentlich verfügbare Internetinformationen zur Katalogisierung und Erstellung großer Daten-Caches ohne eine ausdrückliche vertragliche Vereinbarung mit dem primären Herausgeber der Informationen. Durch diese Caches wird Personen im Rahmen einer Internetsuche die schnelle Auffindung von Daten im Internet ermöglicht. Als Folge hieraus kann es jedoch schwierig oder sogar unmöglich sein, alle „Spuren zu beseitigen.“ Aufgrund des Erfordernisses, dass Datencontroller alle Dritten benachrichtigen müssen, scheint das Recht auf Vergessenwerden von der Annahme auszugehen, dass Unternehmen die Gesamtheit des World Wide Web überblicken und die darin befindlichen Informationen kontrollieren *können* – eine Verpflichtung, die in direktem Widerspruch zur offenen Architektur des Internets steht.
- **Um die Durchführbarkeit des Rechts auf Vergessenwerden zu gewährleisten, darf dessen Auslegung nicht als Verpflichtung der Unternehmen zu einer Handlung ausgelegt werden, die technisch unmöglich ist.** Dementsprechend unterstützt Microsoft die Möglichkeit der betroffenen Personen zur Berichtigung oder Löschung der ihnen gehörenden Daten, soweit dies auf solche Daten beschränkt ist, die ***vom Datencontroller aufbewahrt oder sich unter dessen Kontrolle befinden***, sodass auf die Daten im gewöhnlichen Geschäftsverlauf

innerhalb einer angemessenen Frist, in angemessener Weise zugegriffen werden kann, nachdem die betroffene Person ihr berechtigtes Interesse an den Daten hat nachweisen können.

- Ausnahmen sollten in Fällen möglich sein, in denen Daten für historische, statistische und wissenschaftliche Forschungszwecke, aus Gründen des öffentlichen Interesses, für die Ausübung des Rechts auf freie Meinungsäußerung, die Vertragserfüllung, die Erfüllung regulatorischer Erfordernisse, die Bekämpfung von Betrug und anderen schädigenden Handlungen, die Compliance, die Verteidigung gegen Rechtsansprüche, wegen berechtigter Interessen, für die Vermeidung eines unverhältnismäßigen Aufwands und für den Schutz der Rechte anderer natürlicher oder juristischer Personen aufbewahrt werden müssen. Ferner sollte die Anonymisierung der Daten einer Löschung gleichgestellt werden.

Datenportabilität

- Mit der wachsenden Inanspruchnahme von Online-Dienstleistungen, sozialen Netzwerken und der Cloud-Technologie zur Speicherung aller möglichen personenbezogenen Daten ist es zunehmend wichtiger geworden, dass Nutzer bei Kündigung eines Service ihre Daten mitnehmen können.
- **Microsoft unterstützt nachdrücklich die Forderung, Personen größere Kontrolle über ihre Daten zu geben - eine erhöhte Datenportabilität ist nicht nur für die Nutzer, sondern auch für die Wirtschaft und das gesamte Ökosystem von Vorteil.** Microsoft ist daher der Ansicht, dass die Nutzer Eigentümer ihrer Daten und folglich berechtigt sein sollten, diese zurückzuerhalten. Die Verordnung sollte jedoch der technischen Realität Rechnung tragen, dass die Möglichkeit zum Datenexport nicht unbedingt bedeutet, dass Daten in ihrer gegenwärtigen Form bei anderen Services genutzt werden können. Unternehmen verwenden - abhängig von den beteiligten Technologien, Services und Funktionalitäten - eine ganze Reihe verschiedener Mechanismen zur Ermöglichung des Datenexports, darunter Industriestandardformate, Import/Export-Funktionen und APIs (Application Programming Interfaces), die Dritten eine direkte Verbindung zu den Daten erlauben. Und täglich werden neue Mechanismen erfunden. Daher ist die erfolgreiche Datenübertragung von einem Service auf einen anderen keine leichte Sache. Die Forderung eines einzigen Formats zur Datenübertragung verlangt von Technologieanbietern die Abänderung anderer Aspekte ihrer Produkte und Dienstleistungen, was zu Abstrichen bei der Funktionalität, zu einer geringeren Produktvielfalt und einer insgesamt schlechteren Erfahrung der Nutzer führen kann.
- **Microsoft schlägt eine Lösung vor, die Nutzern die Übertragung der ursprünglich von ihnen geschaffenen Daten gestattet und der Industrie die Entscheidung über die Formate und technischen Einzelheiten** einer Rückgabe der Nutzerdaten an die Nutzer auf der Grundlage einer Reihe technischer und kommerzieller Faktoren sowie unter Berücksichtigung der Benutzerfreundlichkeit und des Vorherrschens eines bestimmten Formats und eines bestimmten Verfahrens überlässt.

Verletzung des Schutzes personenbezogener Daten

- Die Begründung einer Pflicht der Datencontroller zur Meldung schwerwiegender Verletzungen des Schutzes personenbezogener Daten an die zuständigen Behörden und die betroffenen Personen wird zu einem höheren Standard des Datenschutzes in der gesamten Industrie führen. Eine Regelung zur Meldung von Verletzungen des Datenschutzes muss jedoch praktisch umsetzbar sein. Die geplante Verordnung würde Datencontroller auch zur Meldung nicht schwerwiegender Verletzungen des Datenschutzes zwingen. Dieser Ansatz droht die Datenschutzgesetze und die betroffenen Personen mit Meldungen von Verletzungen, die sich schließlich als unwesentlich erweisen, zu überhäufen, was die betroffenen Personen letztlich wiederum dazu veranlasst, die Meldungen einfach zu ignorieren. Es ist beispielsweise nicht sinnvoll, den Fall eines gehackten Online-Computer-Gaming-Accounts, bei dem der Hacker Zugriff auf die Spielergebnisse eines Spielers erhält, in der gleichen Weise zu behandeln, wie eine Verletzung der elektronischen Krankenunterlagen eines Patienten.
- Daher muss die Fristenregelung für die Meldung an eine betroffene Person seitens einer Organisation flexibler ausgestaltet werden, um Ermittlungen, forensische Untersuchungen und Abhilfemaßnahmen durchführen zu können. Microsoft ist der Überzeugung, dass die vorgesehene Meldefrist von 24 Stunden praktisch nicht umsetzbar ist. Aufgrund der Erfahrungen von Microsoft gibt es bei jedem „Verdacht auf eine Verletzung“ einen Zeitraum, in dem der Vorfall stabilisiert und untersucht wird. Microsoft ist vor Abschluss dieser Phase nicht in der Lage, irgendjemanden zu benachrichtigen. Die Feststellung der tatsächlichen Ursache des Vorfalls kann mehrere Tage oder auch einen längeren Zeitraum in Anspruch nehmen, dringende Gegenmaßnahmen zur Stabilisierung des Vorfalls (z.B. Offline-Betrieb des gesamten Systems, Widerruf des Zugriffs und dergleichen), den Abschluss der forensischen Untersuchungen zur Feststellung der betroffenen Daten und der Personen, auf die sich die Daten bezogen, und die Durchführung einer Risikoeinschätzung erfordern. Im Anschluss daran, wenn eine Meldung an die betroffenen Personen erforderlich ist, muss die Kommunikation im Rahmen der Meldung vorbereitet werden, deren korrekte Erstellung üblicherweise ein paar Tage benötigt. Hierzu ein Beispielfall zur Veranschaulichung:

  Der Mitarbeiter einer Organisation hat seinen Laptop verloren oder der Laptop wurde ihm gestohlen (ein leider relativ häufiger Vorfall, von dem die meisten Organisationen betroffen sind). Der Mitarbeiter meldet den Verlust nach Feststellung seinem Vorgesetzten und/oder der Sicherheitsabteilung. Diese Meldung kann im Verlauf des ersten Tages, an dem der Verlust bemerkt wurde, oder auch erst 2-3 Tage nach dem Verlust erfolgen (z.B. wenn sich der Verlust an einem Wochenende ereignete und der Mitarbeiter diesen erst am Montagmorgen bemerkte). Ein Mitglied der Sicherheitsabteilung wird dem Fall zugewiesen, der gemeinsam mit dem Mitarbeiter festzustellen versucht, mit welcher Verschlüsselungsstufe der Computer versehen war und welche Daten sich darauf befanden.

Diese erste Analyse nimmt regelmäßig einen vollen Tag in Anspruch. Wird festgestellt, dass personenbezogene Daten anderer betroffener Personen betroffen waren und dass die Festplatte unverschlüsselt gewesen ist, wird die Datenschutzstelle benachrichtigt und zur Untersuchung des Falles hinzugezogen. Eine Ermittlungs- und forensische Untersuchungsphase wird zur genauen Feststellung eingeleitet, welche personenbezogenen Daten sich konkret auf dem Laptop befanden. Dazu sind in der Regel weitere Befragungen des betreffenden Mitarbeiters, eine Analyse eventuell vorhandener Datensicherungskopien, eine Analyse der damit zusammenhängenden serverseitigen Daten (wie zum Beispiel E-Mail-Server und Kundendatenbanken, von denen der Mitarbeiter möglicherweise örtliche Kopien auf seinem Laptop hatte) erforderlich. Es kann zum Beispiel eine Situation unter Beteiligung einer Spreadsheet-Datei mit personenbezogenen Daten zahlreicher betroffener Personen eintreten, die sich auf dem PC befand, von der es jedoch keine Sicherungskopien gibt. Der Mitarbeiter kann sich jedoch daran erinnern, vor einiger Zeit eine Kopie der Datei per E-Mail an einen anderen Mitarbeiter geschickt zu haben. Ein IT-Administrator kann die Datei vielleicht in den an einem Offsite-Standort befindlichen Sicherungskopien des E-Mail-Systems des Unternehmens finden. In der Regel dauert der Abschluss aller Analysen mehrere Tage, möglicherweise auch länger. Erst wenn die Organisation mit Sicherheit festgestellt hat, welche Daten mit Bezug zu welchen betroffenen Personen an der Verletzung beteiligt sind, kann sie mit der Vorbereitung und der Verbreitung der Meldungen beginnen. Das Verfassen und Versenden der Meldung kann, je nach Komplexität und Ausmaß der Verletzung der Datensicherheit, nochmals mehrere Tage in Anspruch nehmen.