

Stellungnahme zum Digital Package Omnibus COM (2025)836

(English version below)

EU-Transparenzregisternummer: 031503449561-38

BUGLAS dankt der Kommission für die Möglichkeit, zu dem Vorschlag für das Omnibus-Paket „Digitales Europa“ Stellung zu nehmen. Wir begrüßen die geplanten Vereinfachungen, insbesondere für KMU. Insgesamt haben die Änderungen bei der Meldung von Datenschutzvorfällen, die Straffung der Datenschutzgesetze und der Abbau bürokratischer Hürden das Potenzial, unseren Mitgliedern zu helfen.

Wir werden uns separat zur Meldung von Cybervorfällen, zur Straffung der Datenschutzgesetze und zu den Datenschutzbestimmungen äußern.

Straffung der Datenschutzgesetze

In der Vergangenheit verursachten die fünf separaten Datenschutzgesetze ([Verordnung über den freien Verkehr nicht personenbezogener Daten](#), [Data Act](#), [Open-Data-Richtlinie](#), [Data Governance Act](#) und die [Datenschutz-Grundverordnung \(2016/679\)](#)) einen erheblichen bürokratischen Aufwand für Unternehmen. Wir begrüßen die Reduzierung auf die Datenschutz-Grundverordnung (2016/679) und den Data Act (2023/2854). Neue Vorschriften sollten bestehende Vorschriften evaluieren und wo möglich den bürokratischen Aufwand reduzieren.

Data Act

Für den Data Act schlagen wir vor, Geräte, die für den Aufbau Telekommunikationsverbindungen und die Nutzung von Telekommunikationsdiensten und telekommunikationsgestützten Diensten erforderlich sind (bspw. Router, Modems, Femtozellen, WLAN-Verstärker und Set-Top-Boxen) ausdrücklich aus der Definition von „vernetzten Produkten“ auszuschließen. Artikel 2 Absatz 5 des Data Acts definiert ein „vernetztes Produkt“ als ein Gerät, das Daten generiert oder sammelt, diese übertragen kann und nicht in erster Linie dazu dient, Daten für Dritte zu speichern, zu verarbeiten oder zu übertragen. In den FAQ der Kommission wird weiter klargestellt, dass Produkte, die hauptsächlich zur Datenspeicherung, -verarbeitung oder -übertragung verwendet werden – wie Server und Router –, von den

Datenaustauschpflichten gemäß Kapitel II ausgenommen sind, es sei denn, sie sind Eigentum des Nutzers oder werden von diesem gemietet oder geleast.

Diese Klarstellung birgt jedoch die Gefahr, die Definition der Verordnung selbst zu schwächen. Artikel 2 Absatz 5 schließt bereits Geräte aus, deren Hauptzweck darin besteht, Daten im Auftrag anderer zu verarbeiten oder zu übertragen. Solche Geräte fallen eindeutig in diese Kategorie von Produkten, die in erster Linie zur Speicherung, Verarbeitung oder Übertragung von Daten verwendet werden, da sie die Kommunikation erleichtern, an der naturgemäß Dritte, wie Internetdiensteanbieter beteiligt sind. Daher sollten solche Geräte weiterhin von der Definition des Begriffs „vernetztes Produkt“ ausgenommen bleiben.

Datenschutzgrundverordnung

Wir begrüßen teilweise die Klarstellung der Definition von personenbezogenen Daten, sodass diese nur dann als personenbezogene Daten angesehen werden können, wenn ein bestimmter Akteur die Möglichkeit hat, eine Person zu identifizieren. Nach dem Fall SRB (C-413/23 P) zur Definition von pseudonymisierten Daten, bei denen die Artikel 13 und 14 der DSGVO weiterhin gelten, wünschen wir uns einen ehrgeizigeren Vorschlag der Kommission. Wir begrüßen, dass die Empfänger der pseudonymisierten Daten ohne Möglichkeit der Re-Identifizierung nicht unter die Verpflichtungen der DSGVO fallen. Wir würden eine ähnliche Ausnahme auch anonymisierte Daten, bei denen eine Re-Identifizierung unmöglich ist, sowie für die andere Partei bevorzugen. Dabei ist es wichtig, dass die verarbeitende Partei kein Interesse daran hat, die Person zu identifizieren.

Der Vorschlag für Artikel 12 DSGVO enthält eine Schutzklausel, um den Verantwortlichen vor unbegründeten oder übermäßigen Datenanfragen der betroffenen Person zu schützen, indem eine angemessene Gebühr für den Verwaltungsaufwand verlangt wird. BUGLAS hält diese Schutzmaßnahme für unzureichend. Die Pflicht zur Bereitstellung von Datenschutzhinweisen sollte auf die wesentlichsten Informationen beschränkt werden, vor allem, um deren Länge zu begrenzen und eine einheitliche Umsetzung in der Praxis zu fördern. Datenschutzhinweise sind aufgrund umfangreicher inhaltlicher Anforderungen oft übermäßig lang. Infolgedessen gehen Genauigkeit und Vollständigkeit häufig zu Lasten der Transparenz, Verständlichkeit und Lesbarkeit. In der Praxis werden sie aufgrund ihrer Komplexität und übermäßigen Länge von den betroffenen Personen selten gelesen. Eine Vereinfachung der vorgeschriebenen Angaben wäre

daher sehr wünschenswert und würde die Klarheit und Transparenz für die Nutzer erheblich verbessern.

BUGLAS schlägt vor, Artikel 26 DSGVO bezüglich gemeinsamer Verantwortlicher vollständig zu streichen. Die Ausarbeitung und Pflege solcher Vereinbarungen erforderten einen erheblichen Aufwand, insbesondere bei Vereinbarungen mit mehreren Parteien. Darüber hinaus ist ihr Anwendungsbereich unklar und in der Praxis schwer zu handhaben. In der Praxis kann bereits die bloße Angleichung, an die von einem Dritten festgelegten Zwecke und Mittel zu einer gemeinsamen Verantwortlichkeit führen, selbst wenn Dienstleistungen extern in Auftrag gegeben werden. Da jede Partei bereits bestehenden Datenschutzverpflichtungen unterliegt, bietet eine gemeinsame Verantwortlichkeit keinen zusätzlichen Nutzen, erfordert aber einen übermäßigen bürokratischen Aufwand. Hiermit würde gleichzeitig das erklärte Ziel der Kommission, Unternehmen von übermäßiger Bürokratie zu entlasten, gefördert.

Für Artikel 30 DSGVO schlagen wir vor, die Verpflichtung zur Aufzeichnung von Verarbeitungsvorgängen, die ein sehr geringes Risiko darstellen, im Verzeichnis der Verarbeitungstätigkeiten zu streichen. Die Verpflichtung zur Dokumentation aller Datenverarbeitungsvorgänge, einschließlich solcher, die nur ein minimales Risiko darstellen, verursacht einen erheblichen Verwaltungsaufwand, ohne einen nennenswerten Nutzen zu bieten. Für Verarbeitungen mit geringem Risiko sollten die vorgeschriebenen Mindestangaben erheblich vereinfacht oder vorzugsweise ganz gestrichen werden.

Cookies

Wir befürworten eine größere Erleichterung für Verbraucher bei der Auswahl ihrer Datenschutzeinstellungen in Bezug auf Cookies (ePrivacy-Richtlinie 2002/58/EG). Die bestehenden Vorschriften sind einfach nicht praktikabel, und Verbraucher klicken oft einfach auf die Standardoption, ohne eine fundierte Entscheidung zu treffen. Der vorgeschlagene „Ein-Klick“ für Cookies für Verbraucher, der mindestens sechs Monate lang gültig sein muss, wird die Benutzererfahrung verbessern und gleichzeitig Reibungsverluste auf Websites verringern.

Der Vorschlag einer „Whitelist“ für die Bereitstellung von Diensten wie Statistiken und aggregierten Messungen ohne Auswirkungen auf die Privatsphäre der Nutzer ist ein sinnvoller

Vorschlag zum Schutz privater Daten, ohne dass Unternehmen übermäßig strenge Verpflichtungen auferlegt werden. Es ist jedoch unklar, wie die Cookie Einstellungen der Nutzer gespeichert werden sollen.

Meldung von Cybervorfällen

Die Vereinfachung der Meldung von Datenschutzvorfällen an die Europäische Agentur für Cybersicherheit (ENISA) verringert den Verwaltungsaufwand für unsere Mitglieder. Die Meldung an nur eine Stelle hilft insbesondere KMU mit begrenzten Ressourcen und gewährleistet eine schnelle Meldung von Vorfällen.

Während der aktuelle Vorschlag für ein digitales Omnibuspaket erhebliche Vereinfachungen für die Meldung von Cybervorfällen vorsieht, birgt die Absicht der Kommission, neue Vorratsdatenspeicherungspläne voranzutreiben, die Gefahr einer erhöhten Verwaltungslast für Telekommunikationsanbieter. Die Pläne Deutschlands, kurz vor der Veröffentlichung eines europäischen Vorschlags zur Vorratsdatenspeicherung ein nationales Vorratsdatenspeicherungsgesetz einzuführen, erschweren die Bemühungen um die Einhaltung der Vorschriften, trotz der behaupteten Vereinfachungsanforderungen.

NIS-2-Richtlinie

Wir unterstützen die vorgeschlagene Verlängerung der Meldefrist für Vorfälle gemäß Artikel 23 Absatz 4 (b) der NIS-2-Richtlinie von 72 auf 96 Stunden. Allerdings halten wir diese Verlängerung für unzureichend. Die ursprüngliche Frist für die Frühwarnmeldung sollte von 24 auf 48 Stunden verlängert werden. Bei Vorfällen, die außerhalb der Bürozeiten am Wochenende auftreten, kommt die zusätzliche Zeit insbesondere KMU zugute, die nicht über rund um die Uhr verfügbare Mitarbeiter verfügen. Im Falle einer Datenverletzung werden alle Ressourcen benötigt, und Meldepflichten stellen eine zusätzliche Belastung dar, ohne dass der Vorfall gelöst wird. Eine Verlängerung der 96-Stunden-Frist gemäß Artikel 23 Absatz 4 (b) und eine Verlängerung auf 48 Stunden gemäß Artikel 23 Absatz 4 (a) würden KMU dabei helfen, den

Vorfall zu melden und sich auf die Suche nach einer Lösung zu konzentrieren, insbesondere wenn Vorfälle an Wochenenden oder Feiertagen auftreten.

Fazit

BUGLAS würdigt die Bemühungen der Kommission, die Regulierung im digitalen Bereich zu reduzieren und zu vereinfachen. Die Harmonisierung oft komplexer und sich überschneidender Vorschriften war längst überfällig. Ausnahmen für KMU von bestimmten Verpflichtungen sind sinnvoll und praktikabel. Künftige Vorschriften sollten nationale und europäische Vorschriften harmonisieren und gleiche Wettbewerbsbedingungen gewährleisten.

-English version-

Position Paper Digital Package Omnibus COM(2025)836

EU transparency register number: 031503449561-38

BUGLAS thanks the Commission for the opportunity to comment on the proposal for Digital Package Omnibus. We welcome the planned simplifications, especially for SMEs. Overall, the changes in data protection incidents reporting, the streamlining of data laws and the reduction of bureaucratic hurdles have the potential to assist our members.

We will comment on the reporting of cyber incidents, the streamlining of data laws and privacy regulations separately.

Streamlining of data laws

In the past the five separate data laws ([Free Flow of Non-personal Data Regulation](#), [Data Act](#), [Open Data Directive](#), [Data Governance Act](#) and the General Data Protection Regulation) created a substantial bureaucratic burden for companies. We welcome the reduction to just the [General Data Protection Regulation \(2016/679\)](#) and the Data Act (2023/2854). New regulations should evaluate existing regulations and reduce bureaucracy where possible.

Data Act

For the Data Act, we propose explicitly excluding devices that are necessary for establishing telecommunications connections and using telecommunications services and telecommunications-based services (e.g. routers, modems, femtocells, Wi-Fi amplifiers and set-top boxes) from the definition of ‘connected products’. Article 2(5) of the Data Act defines a ‘connected product’ as a device that generates or collects data, can transmit it, and is not primarily intended to store, process or transmit data for third parties. The Commission's FAQ further clarifies that products primarily used for data storage, processing or transmission – such as servers and routers – are exempt from the data sharing obligations under Chapter II, unless they are owned, rented or leased by the user.

However, this clarification risks weakening the Regulation's own definition. Article 2(5) already excludes devices whose main purpose is to process or transmit data on behalf of others. Such equipment clearly falls into this category of products primarily used for data storage, processing, or transmission, as they facilitate communications that inherently involve third parties like internet service providers., such devices should continue to be excluded from the definition of "connected product."

The general data protection regulation

We welcome, in part, the clarification of the definition of personal data, so that it can only be considered personal data if a specific actor has the ability to identify a person. Following the SRB case (C-413/23 P) on the definition of pseudonymised data, to which Articles 13 and 14 of the GDPR continue to apply, we would like to see a more ambitious proposal from the Commission. We welcome the fact that recipients of pseudonymised data without the possibility of re-identification are not subject to the obligations of the GDPR. We would also prefer a similar exemption for anonymised data where re-identification is impossible, as well as for the other party. It is important that the processing party has no interest in identifying the person.

The proposal for Article 12 GDPR contains a safeguard clause to protect controllers from unfounded or excessive data requests from data subjects by requiring a reasonable fee for the administrative burden. BUGLAS considers this safeguard measure to be insufficient. The obligation to provide data protection notices should be limited to the most essential information, primarily in order to limit their length and promote uniform implementation in practice. Data protection notices are often excessively long due to extensive content requirements. As a result, accuracy and completeness often come at the expense of transparency, comprehensibility and readability. In practice, due to their complexity and excessive length, they are rarely read by the data subjects. Simplifying the required information would therefore be highly desirable and would significantly improve clarity and transparency for users.

BUGLAS proposes that Article 26 of the GDPR concerning joint controllers be deleted in its entirety. The drafting and maintenance of such agreements requires considerable effort,

particularly in the case of agreements involving multiple parties. Furthermore, their scope of application is unclear and difficult to manage in practice. In practice, simply aligning with the purposes and means determined by a third party can lead to joint responsibility, even if services are outsourced. Since each party is already subject to existing data protection obligations, joint responsibility offers no additional benefit but requires excessive bureaucracy. This would also promote the Commission's stated goal of relieving companies of excessive bureaucracy.

For Article 30 GDPR we propose to remove the requirement to record processing operations that pose a very low risk in the record of processing activities. Requiring documentation of all data processing activities, including those that involve only minimal risk, creates substantial administrative burden without providing any meaningful benefit. For low-risk processing, the mandatory minimum information should be significantly streamlined or, preferably, eliminated entirely.

Cookies

We are in favour of the greater ease for consumers to choose their privacy settings regarding cookies (ePrivacy Directive 2002/58/EC). The existing rules are simply impractical, and consumers often just click the default option without making an informed choice. The proposed “single-click” for cookies for consumers that must be respected for a minimum of six months will make the user experience better while simultaneously reducing friction on websites.

The proposal of a “whitelist” for the provision of services such as statistics and aggregated measurements without impacting users’ privacy is sensible proposal to protect private data without overprotective obligations for businesses. It is, however, unclear how companies are supposed to save the consumer’s choices regarding their use of cookies.

Reporting of cyber incidents

The streamlining of the reporting of data protection incidents to the European Agency for Cybersecurity (ENISA) reduces the administrative burden for our members. Reporting to only

one entity especially helps SMEs that have limited resources and ensure fast reporting of incidents.

While the current digital package omnibus proposal introduces significant simplifications for cyber incident reporting, the Commission's intention to advance new data retention plans risks increasing the administrative burden on telecommunications providers. Germany's plans to introduce a national data retention law shortly before the release of a European data retention proposal complicate compliance efforts, despite claims of simplification requirements.

NIS 2 Directive

We support the proposed extension from 72 to 96 hours for incidents reporting under Article 23 4 (b) of NIS2. However, we regard the extension as insufficient. The initial early warning reporting deadline should be extended from 24 to 48 hours. For incidents occurring outside office hours on the weekend, additional time especially helps SMEs that do not have 24/7 active staff. In the case of data breach all resources are needed, and reporting obligations add an additional burden without solving the incident. An extension of the 96 hours deadline under article 23 4 (b) and an extension to 48 hours under Article 23 4 (a) would help SMEs to report the incident and being able to focus on finding a solution, especially when incidents occur on weekends or holidays.

Conclusion

BUGLAS acknowledges the Commission's efforts to reduce and simplify digital regulation. The harmonization of often complex and duplicate regulations was overdue. Exemptions for SMEs from certain obligations are sensible and practical. Future regulations should harmonize national and European regulations and ensure a level playing field for competition.