Bitkom on the reform of cookie and device-access rules

as part of the Digital Omnibus

bitkom

At a glance

Bitkom on the reform of cookie and device-access rules

Initial position

The Digital Omnibus is intended to simplify Europe's digital legal framework. There is a particular need for action regarding access to terminal equipment, cookies, and comparable technologies. The current rules are fragmented and formalistic, and lead to excessive consent requests. This affects not only online advertising and media, but also cybersecurity, industry, mobility, connected products, and digital services.

Bitkom rating

The merging of ePrivacy and GDPR rules can create greater coherence. However, it is crucial that device access and comparable technical processes are no longer subject across the board to a prior consent requirement. The objective is a risk-based framework that provides legal certainty for legitimate, low-risk, and security-relevant processing in digital services, connected products, and industrial applications, while at the same time effectively reducing unnecessary consent requests and cookie fatigue.

The most important takeaway

Bitkom supports the objective of simplification, but sees a significant need for improvement. Our paper outlines the following compromise positions:

- **Regulate device access on a risk-based basis**

  Access to terminal equipment should not, as a rule, require consent. All legal bases under Article 6 GDPR, in particular legitimate interests, must remain genuinely available.

- **Expand purposes that do not require consent**

  Audience measurement, aggregation, fraud prevention, cybersecurity, product improvement, and core functions in the context of device access – particularly also in digital services, industrial applications, and connected products – should be expressly possible without consent.

- **Do not create new gatekeeper structures**

  Browser-based signals must not lead to parallel consent flows, conflicting preferences, or de facto control by individual intermediaries over digital business models.

Content

Device access is not a niche issue for the digital economy and is not limited to cookies

The European Commission's Digital Omnibus fundamentally pursues the right objective. Europe's digital legal framework should be simplified, harmonised, and made more innovation-friendly. Bitkom welcomes this approach. However, it is crucial that the announced simplification is not watered down during the legislative process, but instead leads to tangible relief, greater legal certainty, and a consistently risk-based legal framework.

The need for action is particularly evident with regard to access to terminal equipment, cookies, and comparable technologies. Politically, these issues are often reduced to online advertising or media services. In reality, however, they affect almost all sectors that use websites, apps, connected products, or digital services – from media, retail, and platforms to cybersecurity and industrial IoT applications, as well as automotive, energy, and mobility.

Today, access to terminal equipment is the technical basis for numerous legitimate and, in some cases, security-relevant functions: audience measurement, fraud prevention, IT security, error analysis, software updates, product improvement, predictive maintenance, fleet management, and road safety. A regime that continues to subject this diversity across the board to a prior consent requirement remains formalistic and fails to achieve the goal of practical, risk-based regulation.

Device access concerns security, mobility, and industry – example: connected vehicles

The debate must not be understood as a mere «cookie debate". Access to terminal equipment also significantly affects connected vehicles, industrial devices, machinery, sensors, and other connected products. In precisely these areas, a device-access regime based solely on consent can create significant risks for innovation, product safety, and road safety.

Modern driver assistance systems and automated driving systems rely on real-world traffic data. These data are not used for advertising or surveillance, but for accident prevention, system validation, product monitoring, quality improvement, and the detection of rare safety-critical situations. If substantial parts of the available data may not be used due to formal consent requirements, systematic data gaps arise. The result is not greater data protection, but potentially lower system robustness and reduced road safety.

In addition, there is the multi-user reality of connected products. Vehicles, machines, or devices are often used by owners, keepers, family members, employees, tenants, fleet users, or workshops. At the same time, other persons may inevitably be affected from a technical perspective. Prior individual consent management for all potentially affected persons is practically impossible to implement in such constellations.

A practicable legal framework must therefore differentiate between the end user, data subject, owner, keeper, contracting party, subscriber, and actual user. In practice, it is

often the contracting party or main user who activates a service, for example the vehicle owner for theft protection, the fleet operator for fleet management, or the keeper for predictive maintenance. A regime that makes such functions dependent on the consent of all possible users is not practicable.

For connected products and vehicles, it should be expressly provided that the concept of the subscriber from Article 5(3) of the ePrivacy Directive is retained, so that the keeper, owner, or contractual main user can continue to activate certain services, provided that these are necessary, proportionate, and transparent, and that the rights of other affected persons are adequately safeguarded. Otherwise, the changes in the Digital Omnibus risk bringing about a significant change and tightening of the legal situation compared with the status quo. This is necessary in particular for theft protection, alarm notifications, vehicle location in the event of loss, maintenance information, breakdown notifications, battery charge status, fleet operations, product safety, and road safety.

The legislator must ensure that device-access rules do not unintentionally render security-relevant processing and processing envisaged by law impossible. At a minimum, an express exemption is required for processing in the public interest, in particular for road safety, product safety, product monitoring, error analysis, and compliance with legal obligations.

A coherent GDPR framework instead of merely shifting the ePrivacy problem

Bitkom generally welcomes the objective of overcoming the current fragmentation between the ePrivacy Directive and the GDPR, and of integrating rules on access to terminal equipment more closely into a uniform data protection framework. However, the decisive factor is the substantive content of the provision.

The proposals to date show that the regulatory approach remains in flux. While the Commission draft and early Council compromises provided for standalone provisions in Articles 88a and 88b GDPR, the second Council compromise shifts central elements into a new Article 8b GDPR. The Cypriot compromise proposal now under discussion would relocate the rules on cookies and terminal equipment more strongly, or even entirely, back into Article 5(3) of the ePrivacy Directive, adding only further exemptions from consent there.

Such a relocation back is not convincing. The integration of personal data-related device access into the GDPR made sense precisely because it can reduce the overlaps between the GDPR and the ePrivacy Directive that have existed for years. The right answer to the weaknesses of the current proposals is therefore not a return to the fragmented ePrivacy regime, but a targeted refinement of the GDPR-based approach.

The central problem is not that device access is to be integrated into the GDPR. Rather, the problem is that the proposed exemptions from the consent requirement remain too narrowly defined. Both the Commission proposal and the second Council compromise essentially maintain a prior consent model and allow access without consent only for limited categories of cases. As a result, the structural problem of the existing ePrivacy framework would not be resolved, but merely continued elsewhere.

A coherent legal framework must follow the logic of the GDPR. This means that device access must not be treated across the board as requiring consent where the underlying purposes are low-risk, security-relevant, technically necessary, anonymised, aggregated, or in the public interest. Instead, all legal bases under Article 6 GDPR, in particular legitimate interest under Article 6(1)(f) GDPR, must be genuinely available.

A blanket priority of consent is incompatible with the risk-based logic of the GDPR

The GDPR is not based on a general reservation of consent. Article 6 GDPR contains several equivalent legal bases which, depending on the purpose, risk, and safeguards, enable the lawful processing of personal data. This system reflects a risk-based approach. A blanket priority of consent for every access to terminal equipment contradicts this fundamental choice.

Device access is not inherently high-risk. Many processing operations are technically necessary, low-risk, or serve security, integrity, and quality-related purposes. These include, in particular, audience measurement and aggregated usage statistics, fraud prevention and traffic validation, IT and platform security, contextual advertising without profiling, product improvement, error analysis, as well as security and quality functions of connected products.

Such operations must remain possible without mandatory consent on the basis of a balancing of interests under Article 6(1)(f) GDPR. Should the legislator nevertheless maintain a catalogue of purposes exempt from consent, this catalogue must be significantly expanded and designed as non-exhaustive. In particular, contextual advertising without profiling, as well as measures to detect and prevent identity fraud, bot traffic, traffic manipulation, and the concealment of user intentions, must be expressly covered.

This applies all the more if consent is to be managed increasingly through central browser or device settings in the future. Such settings can only reflect the diversity of specific usage contexts, services, safeguards, and user expectations to a limited extent. Structurally, they are not designed to take differentiated account of whether a provider uses particularly data-minimising, transparent, or user-friendly procedures. Individual efforts to ensure a particularly data-protection-compliant design would then no longer be reflected in higher consent rates. This weakens incentives for privacy-friendly innovation and may disadvantage precisely those providers that focus on quality, transparency, and purpose limitation.

Such a mechanism also risks entrenching existing market power. Small and medium-sized enterprises in particular cannot compensate for losses of consent or restrictive default settings as easily as providers that rely on purpose-specific, context-related, and legally secured data use for the further development of their products. This concerns, for example, the improvement of digital services, personalised quality functions, or the continuous optimisation of chatbots and other interactive systems that are intended to better reflect customer interests.

A formalistic consent requirement does not lead to better protection of fundamental rights. It produces more banners, more prompts, more patterns of refusal, and greater

legal uncertainty, but not necessarily more transparency, control, or protection. Data protection regulation should therefore be based on actual risks, purposes, and safeguards, not on the mere fact of technical access.

Purposes exempt from consent must not be exhaustive or too narrowly defined

The second Council compromise continues to pursue an approach under which only a limited list of specific purposes is permissible without consent. Such an approach is too static for dynamic digital and industrial applications. It can only incompletely reflect today's practice and is hardly capable of covering future innovations.

A risk-based approach should not operate solely through a narrow positive list. Rather, access to terminal equipment should be permissible where:

- there is a legal basis under Article 6 GDPR, in particular a legitimate interest;
- a legitimate purpose is specifically defined;
- the access is necessary and proportionate;
- no overriding interests or fundamental rights of the data subjects stand in the way;
- appropriate safeguards are in place, in particular data minimisation, purpose limitation, transparency, aggregation, anonymisation, short retention periods, and options to object where appropriate.

Positive lists can be helpful in creating legal certainty for typical low-risk purposes. However, they must not be exhaustive and must not displace access to Article 6 GDPR.

Audience measurement, aggregation, and anonymisation must be expressly enabled

A practicable regulatory framework must ensure that data may be collected without consent for the purpose of immediate anonymisation or aggregation, provided that no personal profiling takes place and the data are not used for other purposes. This must apply not only to audience measurement, but also to the performance measurement of digital advertising, for example to determine whether, how often, and in what environment advertising materials were displayed and whether campaigns can be evaluated in aggregated form. Once effective anonymisation has taken place, aggregates should be freely reusable, as they no longer relate to individuals.

Although the second Council compromise generally recognises aggregated audience measurement as a low-risk purpose, it restricts it too narrowly. By contrast, the performance measurement of digital advertising is not sufficiently clearly recognised as an independent, legitimate, and low-risk use case. Measurement is essentially intended to be carried out for the controller's own use or by a processor. The data are not to be further processed for other purposes, combined with data from other services, or shared with third parties.

This limitation does not reflect market reality. Small and medium-sized enterprises, start-ups, media services, and specialised providers in particular are often unable to conduct audience measurement and digital performance measurement entirely in-house. They depend on specialised service providers. This applies in particular to advertising-financed digital services, where aggregated information on ad delivery, visibility, frequency, campaign performance, fraud prevention, and quality assurance is necessary in order to manage advertising efficiently, verifiably, and in an economically viable manner. The decisive factor should not be how many technical actors are involved in a measurement process, but whether the processing is purpose-bound, minimised, aggregated, anonymised, and subject to appropriate safeguards.

The legislator should therefore clarify that:

- collection for the purpose of immediate anonymisation or aggregation is possible without consent, provided that no personal profiling takes place and the data are not used for other purposes;
- this expressly also applies to audience measurement, aggregated usage statistics, and the performance measurement of digital advertising, insofar as these are purpose-bound, aggregated, or anonymised and do not serve to create personal profiles;
- the use of specialised service providers and processors is expressly permitted;
- appropriate involvement of service providers, advertising partners, and measurement providers remains permissible, provided that the processing is limited to measurement, billing, quality assurance, fraud prevention, or aggregated campaign evaluation and appropriate safeguards are in place;
- effectively anonymised aggregates may be freely reused.

This would reduce cookie fatigue, enable companies to obtain the control and quality information they need, and at the same time safeguard the functioning of advertising-financed digital services without weakening the protection of users.

Fraud prevention and cybersecurity must not depend on prior consent

Fraud prevention and cybersecurity must be possible without prior consent. Companies must be able to detect and defend against attacks, bot traffic, identity misuse, account takeovers, fake accounts, payment fraud, and AI-supported fraud patterns. Requesting consent before carrying out such security measures is impractical and may undermine the security function itself.

Although the Council compromise generally recognises security purposes, it formulates them too narrowly. Security measures do not depend on whether a user has expressly «requested" them. Users rightly expect digital services to be operated securely.

Fraud prevention, attack detection, and abuse prevention are objective security necessities. They protect not only individual user accounts, but also other users,

platform integrity, payment transactions, business processes, and critical digital infrastructures.

The legislator should therefore expressly clarify that device access and comparable technical measures are permissible without consent where they are necessary and proportionate for fraud prevention, abuse detection, bot and spam defence, account and payment security, the integrity and availability of digital services, defence against AI-supported attacks, as well as security analysis and the ongoing adaptation of detection patterns.

Particularly in view of increasingly automated and AI-supported attack methods, a prior consent requirement would not only be ineffective, but would also create security risks.

Avoid contradictions in legal assessment and create facilitations for anonymous and non-personal device data

Anonymous or non-personal device data must not end up being subject to stricter regulation than personal data. This risk arises if personal data-related device access is regulated under the GDPR, while non-personal device data continue to fall under the stricter regime of Article 5(3) of the ePrivacy Directive.

Relocating the rules on cookies and device access back into Article 5(3) of the ePrivacy Directive would not solve this problem, but would tend to entrench it. It would perpetuate the structural separation between personal and non-personal device data and continue to give rise to complex questions of delimitation.

The objective must be a uniform, coherent, and risk-based device-access framework that avoids contradictions in legal assessment between the GDPR and the ePrivacy Directive. Less intrusive processing, such as anonymous telemetry, diagnostic, or security data from industrial and technical systems, must not be subject to stricter requirements than personal data.

The legislator should therefore either design the scope of application in such a way that non-personal device data are also covered coherently, or amend Article 5(3) of the ePrivacy Directive accordingly. The decisive point is that device access should be regulated in a risk-based and practicable manner, irrespective of whether the data relate to an individual.

Cookie fatigue cannot be solved through gatekeepers

A central objective of the reform is to reduce cookie fatigue. Bitkom expressly shares this objective. Users should not be burdened by excessive, repeated, and uninformative requests. However, the right approach is not to shift consent decisions centrally to browser providers or other intermediaries.

The provisions on automated and machine-readable signals envisaged in the Commission proposal and further developed in the Council compromise ultimately mean that online services would have to comprehensively take account of browser-based or intermediary-controlled preference signals. At the same time, larger browser providers would be required to provide the corresponding technical means.

This raises significant practical and competition-related questions. Browser providers could effectively become central control points for the permissibility of digital business models. Decisions on access to users, reach, measurability, and refinancing must not be shifted unilaterally to a small number of technical intermediaries.

It also remains unclear whether browser-based consent and opt-out mechanisms are intended to replace existing website- and app-based mechanisms or merely supplement them. If they were introduced only in addition to existing mechanisms, this would create parallel consent flows with considerable risks of conflicting signals, operational complexity, and additional legal uncertainty. Cookie fatigue would then not be reduced, but supplemented by another technical and legal layer.

In addition, viable automated signals require mature, interoperable, and sufficiently granular standards. They would need to be purpose-specific, revocable, and functional across different technical environments, including mobile apps and app ecosystems in which browsers are not the central intermediary. Without such standards, divergent technical solutions and renewed implementation uncertainty would be likely.

Cookie fatigue must be addressed at its root cause through a clear, risk-based reduction of unnecessary consent requirements, not through the centralisation of consent with browser providers.

Six-month blocking period is impracticable and excessive

The requirement that, after a consent request has been rejected, no new request may be made for the same purpose for at least six months remains particularly problematic. Such a rigid blocking period is hardly manageable in practice and may produce contradictory effects.

In order to recognise a rejection over a period of six months, a technical identifier would often have to be set or stored. This creates the paradoxical result that enforcing a «no cookies" decision may itself require storage on the terminal equipment.

Moreover, usage contexts change. Users may later use a service differently, activate new services, take out a subscription, change devices, or wish to revisit a situational decision. A rigid blocking period is no substitute for good user guidance. It may even prevent meaningful, transparent, and privacy-friendly choices from being offered again in a new context.

Here too, the legislator should rely on transparency, proportionality, and a risk-based approach rather than prescribing rigid time limits.

Possible legislative implementation options

From Bitkom's perspective, an ambitious, coherent GDPR-based approach is preferable. In any event, at least a targeted improvement of the existing proposals is necessary.

Scope of regulation	**Option 1: Ambitious risk-based approach**	**Option 2: Minimum correction of the existing approach**
Cookie-Regime für personenbezogene Daten	Integration into the GDPR with the consistent applicability of all legal bases under Article 6 GDPR, in particular legitimate interests. Device access would therefore not be subject to a blanket consent requirement, but would be assessed on a risk-based basis.	Retention of a specific cookie and device-access regime, but with a significant expansion of the exemptions from the consent requirement, in particular for contextual advertising without profiling, audience measurement, fraud prevention, IT security, product improvement, and security-relevant applications.
Browser-based signals / Article 8b	No browser-based consent as a central regulatory mechanism. At most, a genuine opt-out mechanism for certain processing operations, which would apply only once practicable and interoperable standards are in place.	Deletion or significant limitation of the requirements concerning browser-based consent and preference signals. In particular, browser providers must not become central gatekeepers for digital business models.
Article 5(3) of the ePrivacy Directive	Limitation to non-personal device data only, insofar as no coherent GDPR framework is created; in doing so, no stricter requirements should apply than for personal data.	Amendment of Article 5(3) of the ePrivacy Directive in order to avoid contradictions in legal assessment and to ensure that anonymous, aggregated, or functional device data are not treated more strictly than personal data.

Specific recommendations

Bitkom recommends designing the rules on cookies and device access in the Digital Omnibus on a fundamentally risk-based basis. In particular, the legislator should:

1. clarify that device access does not generally require consent, but can be based on all legal bases under Article 6 GDPR, in particular Article 6(1)(f) GDPR;
2. avoid relocating the rules on cookies and device access back into a fragmented ePrivacy regime and instead refine the GDPR-based approach in a targeted manner;
3. delete Article 88b/8b GDPR, or any successor provision on automated browser or preference signals, or at least limit it in such a way that browser providers do not become central control points for digital business models;
4. delete rigid blocking periods for renewed consent requests or replace them with a flexible, context-specific, and risk-based approach;
5. expressly enable audience measurement, aggregation, and anonymisation without consent, including the use of specialised service providers and processors;
6. expressly recognise fraud prevention and cybersecurity as purposes that do not require consent, including AI-supported fraud detection, bot defence, traffic validation, account and payment security, as well as the detection and prevention of deception regarding identity, user intention, or traffic source;
7. include product improvement, error analysis, product monitoring, research and development, and security functions of connected products in the catalogue of purposes that are exempt from consent or can be based on legitimate interests;
8. create a clear exemption from the consent requirement for data processing in the public interest, in particular road safety, product safety, and compliance with legal obligations;
9. expressly regulate multi-user devices and subscriber constellations, in particular in relation to vehicles, fleets, rental and employment contexts, and connected products;
10. ensure that anonymous or non-personal device data are not subject to stricter rules than personal data, but that risk-appropriate facilitations and exemptions are created for such data;
11. not treat cookie reform as an isolated online advertising issue, but as a horizontal issue for the European economy, industry, mobility, security, and digital sovereignty.

Summary & outlook

The reform of the cookie and device-access regime is a key strategic decision for Europe's digital and industrial competitiveness. It will determine whether Europe creates a modern, risk-based, and innovation-friendly data protection framework, or whether an outdated consent model is merely continued in a new form.

Effective protection of privacy does not require blanket consent for every technical access. It requires clear rules, genuine risk differentiation, transparency, purpose limitation, data minimisation, safeguards, and enforceable rights.

Where high risks exist, consent or another strict justification must be required.

Where processing is low-risk, security-relevant, anonymised, aggregated, or carried out in the public interest, it must be possible without unnecessary banners and without gatekeeper structures.

Europe does not need a mere relocation of the ePrivacy problem. Europe needs a coherent, risk-based legal framework that protects fundamental rights, reduces cookie fatigue, and enables digital innovation across all sectors.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Isabelle Stroot| Head of Data Protection Law and Policy
P +49 30 27576-228 | i.stroot@bitkom.org

Responsible Bitkom Committee
WG Data Privacy