# VATM Position on the Revision of the EU Cybersecurity Act

## Introduction

In an increasingly complex geopolitical environment marked by intensifying cyber threats, digital infrastructure has become a central pillar of Europe's economic security and societal resilience. Electronic communications networks are at the heart of this infrastructure. VATM therefore welcomes the European Commission's efforts to further strengthen cybersecurity at EU level.

At the same time, providers of electronic communications networks already operate within an extensive and evolving cybersecurity framework. The NIS2 Directive, the Cyber Resilience Act, the Critical Entities Resilience Directive, the Cyber Solidarity Act and the coordinated implementation of the 5G Toolbox have significantly expanded regulatory obligations in recent years. Taken together, these instruments form a dense and continuously evolving regulatory landscape in which multiple frameworks apply in parallel, often with overlapping scopes, interdependencies and evolving requirements. This increasing regulatory layering may give rise to legal uncertainty for operators, particularly where obligations are further specified, updated or extended over time. While these instruments pursue important objectives, they have also increased regulatory density and compliance complexity. For infrastructure operators with long investment cycles, such dynamics do not only affect compliance processes but also planning certainty, as evolving or unclear requirements may influence procurement decisions, vendor strategies and financing conditions beyond immediate regulatory costs. The revision of the Cybersecurity Act should therefore enhance coherence and alignment across the existing framework and contribute to greater simplification, legal certainty and predictability for long-term investment decisions, supporting a resilient roll-out of digital infrastructure and reinforcing Europe's digital transformation.

Against this background, the proposal introduces a Trusted ICT Supply Chain Framework under Section IV. This framework constitutes a significant structural extension of EU cybersecurity policy. By enabling the identification of key ICT assets and the designation of high-risk suppliers, it establishes the legal basis for restrictive measures that may directly affect network architecture and vendor ecosystems.

For infrastructure operators, such measures go beyond incremental compliance adjustments. They may require substantial modifications to existing network configurations, adjustments to long-term procurement strategies and the reassessment of established vendor relationships. Even the anticipation of future supplier designations or asset classifications may influence investment decisions and financing conditions before any formal prohibition takes effect.

While VATM supports the objective of enhancing resilience against supply chain risks, cybersecurity regulation must provide legal clarity and predictable conditions for long-term investment in capital-intensive infrastructure. Measures that significantly alter supplier availability or impose replacement obligations require particular attention to proportionality, technical feasibility and adequate transition periods.



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

**Trusted ICT Supply Chain Framework**

**I. Structural Architecture and Allocation of Powers**

The Trusted ICT Supply Chain Framework introduced in Section IV is the central structural element of the proposal. By allowing the identification of key ICT assets and the designation of high-risk suppliers, it creates the basis for restrictive measures that may directly affect vendor ecosystems and infrastructure planning.

This represents a shift from operator-based risk management toward EU-level determinations capable of affecting supplier availability across sectors. Such determinations are capable of reshaping market conditions for infrastructure operators.

For capital-intensive sectors such as electronic communications, this shift has immediate relevance. The prospect of asset classifications or supplier designations alone can influence procurement strategies, long-term contractual commitments and financing conditions.

VATM supports a coordinated European approach to supply chain security. However, where EU-level decisions may significantly affect vendor ecosystems, the framework must ensure clear criteria, procedural transparency and predictable timelines. Without these safeguards, regulatory flexibility risks creating structural uncertainty for infrastructure operators. Given the potential implications for critical infrastructure sectors, the framework should also ensure appropriate consultation with affected industries and relevant stakeholders when defining key ICT assets or considering restrictive measures.

**I.2 Identification of Key ICT Assets and Scope Expansion**

Article 102 (“Identification of key ICT assets”) empowers the Commission to identify specific components or systems as key ICT assets following coordinated risk assessments under Article 99 (“Security risk assessments”). Such identification forms the basis for mitigation measures under Article 103 (“Mitigation measures in the ICT supply chain”) and, in the telecommunications sector, for potential prohibitions under Articles 110 and 111 (“Key ICT assets for mobile, fixed and satellite electronic communications networks” and “Prohibitions for mobile, fixed and satellite electronic communication networks”).

The definition of key ICT assets therefore determines the practical scope of the framework. VATM considers that this step must remain strictly risk-based and proportionate. Components should only be identified as key ICT assets where there is a clear and substantiated link to specific security risks. In our opinion, the designation of Key ICT Assets in Annex II is not risk-based and hence too broad. Asset identification should therefore be closely linked to clearly defined operational risk scenarios and differentiated levels of criticality within network infrastructures. Transparent methodologies are essential to ensure that mitigation measures correspond to the actual threat landscape and the availability of appropriate technical mitigation options. Broad or insufficiently differentiated asset categories risk extending restrictive measures beyond what is necessary to address identified vulnerabilities.



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

This is particularly significant for electronic communications networks. Article 110 confirms that the framework applies across mobile, fixed and satellite infrastructure. While earlier EU discussions focused primarily on mobile networks, the proposal explicitly extends supply chain risk considerations to fixed networks, materially broadening the potential impact of asset identification decisions.

Mobile and fixed networks differ fundamentally in architecture, lifecycle and substitution feasibility. The identification of key ICT assets must reflect these structural differences. A uniform approach risks creating disproportionate operational consequences in certain network segments.

For VATM, asset identification must therefore be transparent, technically justified and sector-sensitive. It should assess substitution feasibility and integration complexity to ensure that resilience objectives are achieved without generating unintended structural uncertainty for infrastructure operators.

**I.3 Designation of High-Risk Suppliers and Legal Certainty**

Article 104 ("Identification of high-risk suppliers") foresees that the Commission may, by means of implementing acts, identify suppliers considered to present a high level of risk to the security of ICT supply chains. Inclusion on such a list may trigger mitigation measures under Article 103 and, in the telecommunications sector, prohibitions pursuant to Article 111.

For infrastructure operators, supplier identification is the most consequential element of the framework. Unlike general compliance obligations, listing a supplier as high risk can directly affect vendor availability and require adjustments to procurement strategies, long-term contractual relationships and financing structures. In this context, further clarification is needed as to how supplier identification would apply to more complex and layered technology ecosystems, including open-source-based solutions and the providers building on or distributing such components. In such cases, the delineation of responsibility between original developers, integrators and distributors may not be straightforward. Ensuring legal clarity on the scope of supplier designation is therefore essential to avoid unintended regulatory uncertainty and to ensure consistent application of the framework.

VATM emphasises that supply-chain security – also mitigating non-technical risks – must primarily be achieved through risk-based technical and organisational measures rather than through supplier exclusion mechanisms that may in practice be driven by (trade) political considerations. Non-technical risks, including undue state influence, sabotage scenarios or covert data access, are not limited to suppliers from particular jurisdictions. Effective mitigation should be risk-based rather than based on fixed or prescriptive requirements. It therefore requires resilient network design, including redundancies, dual-vendor strategies, modern cryptography, zero-trust architectures and other technically verifiable safeguards.

Replacement obligations create new structural dependencies by reducing the effective supplier base to only a very limited number of vendors. Such a regulatory intervention weakens operators' negotiating position, increases concentration in the supply market and raises procurement costs.



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

In addition, the potential market effects of supplier identification should be carefully considered. Where regulatory measures significantly reduce the number of available suppliers for key network components, this may lead to increased vendor concentration and reduced competition in infrastructure markets. A reduced supplier base may weaken the negotiating position of network operators, affect supply security and increase dependency on a limited number of manufacturers.

From VATM's perspective, supply chain security measures should therefore balance security objectives with the need to maintain a diverse and competitive vendor ecosystem. Network resilience is best supported by a combination of risk-based technical safeguards and diversified supplier strategies rather than by structural reductions in vendor availability alone. Where cybersecurity risks are already addressed through recognised certification mechanisms or technical mitigation measures, additional restrictions on supplier availability should be clearly justified and proportionate in order to preserve the value of certification as an internal market instrument and maintain planning certainty for infrastructure investments.

**II. Implications for the Telecommunications Sector**

Articles 110 ("Key ICT assets for mobile, fixed and satellite electronic communications networks") and 111 ("Prohibitions for mobile, fixed and satellite electronic communication networks") translate the general supply chain framework into sector-specific obligations for providers of electronic communications networks.

VATM emphasises that supply-chain security – including the mitigation of non-technical risks – should primarily be achieved through risk-based technical and organisational measures rather than through supplier exclusion mechanisms that may in practice be driven by geopolitical or trade policy considerations. Effective mitigation requires resilient network design, including redundancies, diversified vendor strategies, modern cryptography and other technically verifiable safeguards. Against this background, broad supplier-based prohibitions should be approached with caution, as they risk reducing vendor diversity and creating new structural dependencies.

In particular, Article 111 foresees prohibitions on the use of components from suppliers identified as high risk in key ICT assets of mobile, fixed and satellite networks. The proposal provides, in certain cases, for a replacement period of 36 months. VATM considers such a replacement period to be unfeasible under any circumstances, given the technical and operational complexity of telecommunications network infrastructure.

Components affected by prohibitions are often deeply integrated into network layers and interconnected with adjacent systems. Replacement may require coordinated hardware and software adjustments, testing cycles and reconfiguration across geographically distributed infrastructure. Large-scale replacement with compressed timelines would also place significant pressure on supply chains and technical resources, with a risk of shortages in specialised engineering capacity and vendor support.

Rather than imposing fixed and compressed timelines, any phase-out obligations should be aligned with infrastructure lifecycles and existing contractual and investment cycles. In practice, this would



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

allow for the gradual replacement of affected components at the point of natural renewal, such as during planned upgrades, contract expiries or technology transitions. Such an approach would ensure that security objectives are achieved in a technically feasible and economically sustainable manner, while avoiding unnecessary disruption to ongoing network deployment and modernisation efforts.

In this context, any decision to impose replacement or phase-out obligations should be preceded by a comprehensive market and impact assessment. Such an assessment should evaluate, in particular, the availability of suitable replacement technologies, the capacity of the supplier market to deliver at scale, realistic implementation timelines and the overall cost implications for operators and end-users. It should also assess the impact on the diversity of technology providers in the market, as maintaining a sufficiently broad and competitive vendor ecosystem is a key element of network resilience and supply security. Without such an evidence-based assessment, there is a significant risk that regulatory measures may prove technically unworkable, economically disproportionate or lead to unintended distortions in infrastructure deployment, competition and long-term supply conditions.

Additionally, accelerated replacement requirements could lead to delays in planned network modernisation and the deployment of new technologies, including the transition to 5G Standalone and more advanced network functionalities. The need for operators to replace equipment with similar timeframes would likely result in significant increases in supply-chain cost. In addition, replacement-driven investment cycles may disproportionately affect network development in less densely populated areas, potentially slowing deployment and widening existing regional gaps.

While mobile network operators have already addressed supply chain risk mitigation in the context of the 5G Toolbox, the extension of this framework to fixed networks represents a significant shift. Fixed access and aggregation layers often involve longer lifecycles and different integration constraints. A uniform replacement timeline may therefore have differentiated impacts across network types.

Replacement obligations of this scale would also involve substantial costs. The European Commission has estimated the cost of 5G supplier replacement at approximately EUR 10–13 billion; however, this figure appears to rely on limited operator input and may not fully capture the technical and operational complexity of infrastructure replacement. Replacement costs are also unlikely to be evenly distributed across Member States and may create significant financial pressure in some markets, potentially leading to higher consumer prices.

In addition, the proposal does not foresee any mechanism to address the financial impact of mandatory replacement obligations. The forced removal of lawfully acquired and operational network components before the end of their economic lifetime may result in substantial asset write-offs for operators. From VATM's perspective, such measures raise important questions of proportionality and investment protection. Where regulatory measures require the premature replacement of functioning infrastructure, the financial implications for operators should be carefully considered in the design and implementation of the framework.



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

### III. Governance, Investment Stability and Coherence

Decisions under Articles 99 to 104 – in particular the identification of key ICT assets and high-risk suppliers and their subsequent updates – may have direct implications for procurement strategies, long-term contractual commitments and capital allocation in the telecommunications sector.

In infrastructure markets characterised by long investment cycles and intensive rollout activity, regulatory predictability is essential. Obligations arising from supplier identification or asset classification may require operators to reallocate capital and adjust long-term vendor strategies. Where transition periods are limited or where the scope of obligations evolves over time, uncertainty may extend beyond immediate compliance costs and influence broader investment decisions.

Greater precision in key regulatory concepts is essential. For example, the identification of key ICT assets under Article 102(2)(a) should take into account the specific use case and deployment environment in which components are operated, rather than relying on overly broad or abstract classifications. Similarly, the scope of mitigation measures under Article 103 requires further clarification, particularly regarding the extent to which different types of infrastructure or actors fall within its application.

Infrastructure deployment depends on stable planning horizons and financing conditions. Uncertainty regarding future restrictions or replacement requirements may affect risk assessments and rollout prioritisation. In such circumstances, operators may adopt more cautious investment strategies, potentially slowing network expansion or redirecting resources from innovation and deployment toward compliance-driven restructuring.

Moreover, the proposal foresees regular updates of supplier designations under Article 104(9). Greater clarity is needed regarding the frequency, criteria and procedural safeguards of such updates. Without predictable update cycles and sufficient lead times, operators may face continuous regulatory uncertainty, which can undermine long-term planning and investment decisions.

From an investment perspective, regulatory approaches that significantly reduce supplier diversity may introduce new structural dependencies and increase exposure to supply-side risks. Ensuring that security objectives are pursued through a balanced combination of technical safeguards and proportionate regulatory measures is therefore essential to maintain both resilience and competitive market structures. This underlines the importance of maintaining a risk-based and proportionate approach, in which security measures are closely linked to concrete threat scenarios and operational contexts, rather than driven by broad or static classifications.

At the same time, the European Commission has proposed the Digital Networks Act with the objective of accelerating the deployment of high-capacity networks and strengthening Europe's digital competitiveness. VATM therefore considers it essential that the implementation of the CSA, once adopted, safeguards the investment incentives underpinning these objectives. Cybersecurity measures and connectivity ambitions should be aligned so that resilience requirements reinforce, rather than inadvertently weaken, long-term infrastructure development in the EU.



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

**IV. Role and Mandate of ENISA**

VATM recognises the value of a strong and technically competent EU cybersecurity agency. A coordinated European approach can contribute to consistency and reduce fragmentation across Member States. At the same time, the scope of ENISA's involvement should be clearly defined. Where assessments under Articles 99 and 102 form the basis for asset identification or supplier listing, the respective responsibilities of the Commission, ENISA and national authorities must remain transparent and well delineated.

For operators, clarity regarding the role of ENISA is important to avoid duplication of reporting or assessment obligations under existing frameworks, including NIS2. Any expansion of tasks should be aligned with existing cybersecurity governance structures and should not result in parallel or overlapping compliance processes.

**V. European Cybersecurity Certification Framework**

The proposal also revises elements of the European cybersecurity certification framework. Certification schemes can contribute to enhancing trust, transparency and comparability of security requirements across the internal market. In principle, a harmonised EU-level approach may reduce fragmentation and provide clarity for market participants.

However, certification requirements must be carefully aligned with existing obligations under other EU instruments, in particular the Cyber Resilience Act and the NIS2 Directive. Overlapping or duplicative requirements risk increasing administrative complexity without delivering security benefits. This concern is particularly relevant for telecommunications providers, which are already subject to extensive cybersecurity, risk-management and audit obligations under NIS2 and, in many cases, additional recognised standards such as ISO 27001.

To preserve the integrity of the internal market, the revised CSA must be closely aligned with existing cybersecurity frameworks and avoid duplicative obligations. Overlapping supervisory, audit and reporting requirements should be prevented where equivalent controls are already fulfilled under NIS2 or sector-specific telecommunications rules. Consistent implementation across Member States is equally important, as national gold-plating would undermine harmonisation and reintroduce fragmentation.

For operators of electronic communications networks, it is essential that any certification schemes remain proportionate and clearly defined in scope. Certification should support risk management and procurement processes rather than create additional layers of regulatory uncertainty. In particular, care should be taken to avoid unnecessary certification obligations for software tools and systems developed in-house and used exclusively for internal network operation. Where such systems are developed and deployed within already regulated and audited environments, additional certification requirements may create significant administrative burden without substantially enhancing security outcomes. VATM therefore calls for an explicit exemption from additional ECCF product, process and service certification requirements for ICT products, services and processes that are developed and used



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

exclusively for internal operational purposes by entities already subject to NIS2 cybersecurity obligations, where such tools are not placed on the market and are operated within already audited and secured environments.

From VATM's perspective, the regulatory framework should clearly distinguish between ICT products placed on the market and systems developed and used internally by operators for the operation of their networks. Where such systems are already subject to the cybersecurity requirements established under NIS2, the need for additional certification obligations under the European Cybersecurity Certification Framework should be carefully assessed.

**VI. Proportionality, Enforcement and Sanctions**

Article 115 ("Penalties") requires Member States to establish rules on penalties applicable to infringements of obligations under the Regulation. Effective enforcement is an essential component of any cybersecurity framework and contributes to consistent application across the EU.

At the same time, electronic communications operators are already subject to extensive cybersecurity obligations under NIS2 and corresponding national implementing measures. In addition, a growing number of EU legislative instruments, including the Data Act and the proposed Digital Networks Act, introduce further requirements relevant to network operation, security and data governance. The interaction between these frameworks and the enforcement regime under the Cybersecurity Act therefore requires careful coordination.

Without clear alignment, there is a risk of overlapping or even conflicting obligations and sanctioning regimes, which may lead to legal uncertainty for operators. This includes, in particular, questions regarding the relationship between horizontal and sector-specific legislation and the determination of which framework applies in a given case. Greater transparency on the interaction and hierarchy of applicable rules is therefore essential to ensure legal certainty and consistent enforcement.

From VATM's perspective, penalties under the CSA should remain proportionate to the nature and gravity of the infringement and take into account the specific characteristics of infrastructure sectors operating within complex technical environments and long integration cycles. Enforcement mechanisms should not result in overlapping or duplicative sanctioning exposure where obligations intersect across regulatory frameworks.

Clear delineation of responsibilities between competent authorities and coordinated supervisory practice will be essential to avoid inconsistent enforcement approaches. Where CSA obligations interact with existing cybersecurity requirements, supervisory alignment can contribute to predictability and reduce unnecessary administrative burden for operators.

**Conclusion**

The revision of the Cybersecurity Act represents an important opportunity to strengthen the resilience of Europe's digital infrastructure and to address evolving risks in ICT supply chains. VATM supports the



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General

objective of enhancing cybersecurity at EU level and recognises the need for a coordinated European approach in this area.

At the same time, the proposed framework introduces far-reaching structural changes with direct implications for network deployment, investment planning and supplier ecosystems in the telecommunications sector. Therefore, it is essential that cybersecurity measures are designed in a manner that ensures legal clarity, proportionality and predictability for infrastructure operators.

Supply-chain security should be pursued primarily through risk-based technical and organisational measures that are closely aligned with concrete threat scenarios and operational realities. Approaches based on broad supplier exclusion mechanisms risk reducing vendor diversity, creating new dependencies and generating unintended consequences for competition, investment and network resilience.

Furthermore, the interaction of the Cybersecurity Act with existing and forthcoming EU legislative frameworks requires careful coordination. Avoiding regulatory overlap, ensuring consistent application across Member States and providing clarity on the relationship between horizontal and sector-specific rules will be critical to reduce legal uncertainty and administrative burden.

Finally, the implementation of the Cybersecurity Act should be aligned with the EU's broader connectivity and competitiveness objectives, including those pursued under the proposed Digital Networks Act. Cybersecurity and infrastructure policy must reinforce each other to support the timely deployment of high-capacity networks and the long-term resilience of Europe's digital ecosystem.

VATM therefore encourages a balanced and proportionate approach that strengthens security while preserving investment incentives, technological diversity and the functioning of competitive markets.

VATM represents Germany's leading telecommunications companies, uniting around 200 network operators, service providers, and suppliers — many of them active at the regional level. The association also speaks for key investors driving the rollout of fibre networks across Germany.VATM members serve 80 percent of all fixed-line customers and nearly all mobile customers outside Deutsche Telekom. Since the liberalization of the market in 1998, competitors in both fixed and mobile segments have invested around €127 billion. Today, they are the principal investors in the fibre-to-the-home (FttH) deployment in Germany, providing 86 percent of all gigabit-capable connections currently in use.



Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de

Präsidium: Valentina Daiber (Präsidentin), Wolfram Rinner (Vizepräsident), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Rickmann v. Platen • Geschäftsführer: Dr. Frederic Ufer

C2 General