STATEMENT

On the ePrivacy Derogation ("Chat Control") and the Negotiations on the Child Sexual Abuse Regulation

14 September 2026

Prepared and led by BlackVogel Consulting

With the support of Blockchain for Europe

I. Summary

On 9 July 2026, the European Parliament considered, at second reading, the Council position reinstating the derogation from Directive 2002/58/EC established by Regulation (EU) 2021/1232, which permits providers of number-independent interpersonal communications services to voluntarily scan private communications for child sexual abuse material. A majority of those voting supported outright rejection (314 votes to 276, with 17 abstentions), but rejection required an absolute majority of 360 Members and therefore failed.[1] The chamber then assembled the absolute majority needed to amend the text, adopting among other changes the exclusion of communications to which end-to-end encryption is, has been or will be applied. The Council approved the amended rules on 23 July 2026.[2] The derogation, which had lapsed on 3 April 2026 following Parliament's rejection of an extension in March, is thereby reinstated in amended and narrowed form until 3 April 2028.

The signatories of this statement do not question the objective of protecting children online, which is a common policy objective that we fully support. However, it is precisely because that objective is so serious that it must be pursued through measures that are effective, targeted, and compatible with the Charter of Fundamental Rights of the European Union. This statement distinguishes throughout between three different elements: the generalised, indiscriminate and suspicionless scanning of private communications, which it opposes; targeted detection subject to judicial safeguards, which it supports; and the removal of known illegal material from publicly accessible services, which it urges. Only the first is in contention. This statement sets out the concerns, legal, technical, and institutional, and presents concrete alternatives for the negotiations on the permanent Regulation laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final) resuming now in

[1]European Parliament, press release, "Combating child sexual abuse: support for a more limited ePrivacy derogation", 9 July 2026, recording the rejection vote (314 in favour, 276 against, 17 abstentions, against a required absolute majority of 360), the adoption of amendments including the exclusion of communications to which end-to-end encryption is, has been or will be applied, and the failure of a motion to reject the amended position (276 in favour, 286 against, 30 abstentions).

[2]Regulation (EU) 2026/1881 of the European Parliament and of the Council of 24 July 2026 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, OJ L, 2026/1881, 28.7.2026. See also Council of the European Union, press release, "Fighting child sexual abuse online: interim measure protecting children now reinstated", 23 July 2026.

autumn 2026. The same principles should guide the assessment of any further initiatives on the protection of children online that the institutions may bring forward.

II. Background & Timeline of the process in the European Union

Regulation (EU) 2021/1232 introduced a temporary derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC (the ePrivacy Directive), allowing, but not obliging, communication providers to apply technologies to detect child sexual abuse material and the solicitation of children in private communications, to report it, and to remove such material. The derogation was conceived as a bridge to a permanent framework and was extended pending agreement on the proposed Child Sexual Abuse Material (CSAM) Regulation.

- **26 March 2026:** Parliament rejected the proposed extension by 311 votes against, 228 in favour, with 92 abstentions, closing its first reading. The existing derogation expired on 3 April 2026. (europarl.europa.eu, press release of 25/26 March 2026, "Child sexual abuse online: voluntary detection measures will not be extended")
- **2 July 2026:** The Council adopted a new position intended to reinstate the derogation until 3 April 2028. (consilium.europa.eu, press release of 2 July 2026, "Council moves to reinstate interim measure to combat child sexual abuse online")
- **7 July 2026:** Parliament approved an urgent procedure (331 votes to 304, with 11 abstentions), returning the file to plenary without renewed committee scrutiny.
- **9 July 2026:** Parliament considered the Council position at second reading. An absolute majority of 360 Members was required to reject or amend it. The motion to reject received 314 votes in favour, 276 against, with 17 abstentions: a simple majority, short of the required 360. Parliament then adopted amendments to the Council position, among them the exclusion of communications to which end-to-end encryption is, has been or will be applied. A motion to reject the amended position also failed (276 in favour, 286 against, 30 abstentions), closing the second reading. (europarl.europa.eu, press release of 9 July 2026, "Combating child sexual abuse: support for a more limited ePrivacy derogation")
- **23 July 2026:** The Council approved the rules as amended by Parliament, confirming that the interim measure is reinstated until 3 April 2028 and that the amended rules would be published in the Official Journal and enter into force three days later. (consilium.europa.eu, press release of 23 July 2026, "Fighting child sexual abuse online: interim measure protecting children now reinstated")
- **September 2026:** According to reporting and a Council Presidency note of 10 September 2026, the European Parliament's shadow rapporteurs are expected to meet on 15 September, a further interinstitutional technical meeting is scheduled for 18 September, EU Ambassadors are set to be consulted on 23 September in the COREPER, and the sixth political trilogue on the permanent Child Sexual Abuse Regulation is to take place on 29 September, where the Presidency seeks general political agreement on detection obligations.

The result is double-edged. A measure the Parliament had rejected four months earlier re-entered into force although a majority of Members voting supported, once again, its rejection; procedure and timing carried it past that majority. At the same time, the chamber found the votes needed to narrow the text and to shield encrypted communications: a partial self-defence that now frames the negotiations on the permanent Regulation, where the decisive open question is the design of detection itself.

III. Concerns

1. Institutional integrity

Confidence in the EU regulatory framework rests on the integrity of the process that produces it. Where the threshold to block legislation is set above the threshold to adopt it, and where the decisive vote is timed for a sitting at which the majority that previously rejected the text foreseeably cannot be assembled, the outcome reflects arithmetic as much as deliberation. Whatever the merits of the underlying file, the precedent, that a text rejected by Parliament may be returned under an urgent procedure bypassing committee scrutiny and carried past a majority of those voting, weakens the institution whose scrutiny gives EU legislation its legitimacy. That the chamber salvaged substantive amendments does not cure the manoeuvre; it shows what the manoeuvre risked foreclosing. This precedent will not remain confined to this file.

The Union has faced this manoeuvre before

In 2005, the Council adopted its common position on the directive on computer-implemented inventions as an "A-item" without debate, over the requests of several Member States to reopen discussion, and after the Commission declined the Parliament's committee request to restart the procedure, relying, as here, on the second-reading rule under which rejection requires an absolute majority while adoption requires none.[3] On that occasion, the Parliament answered the manoeuvre by rejecting the text at second reading by 648 votes to 14, the first outright rejection of a directive at second reading in the Parliament's history, and the file died.

Two lessons follow. First, the threshold is demanding yet within reach where the chamber is present and mobilised; on 9 July the chamber itself proved as much, assembling the absolute majority to amend even as rejection fell short. Second, the Court of Justice has

[3]Proposed Directive on the patentability of computer-implemented inventions (2002/0047(COD)). The Council adopted its common position on 7 March 2005 as an "A-item" without debate, over requests by several Member States to reopen discussion, and after the Commission declined to act on the request of the Parliament's Legal Affairs Committee (adopted 19–1 on 2 February 2005) to restart the procedure. On 6 July 2005 the Parliament rejected the text at second reading by 648 votes to 14, with 18 abstentions, the first outright rejection of a directive at second reading.

long held that the Parliament's effective participation in the legislative process is an essential procedural requirement whose disregard renders the resulting act void[4], the constitutional principle that procedure exists to secure deliberation rather than to substitute for it.

2. Fundamental rights and the balancing of rights

The confidentiality of communications is protected by Article 7 of the Charter, and the protection of personal data by Article 8. These are not absolute rights, and the protection of children engages rights of equal constitutional rank, including Article 24 of the Charter. Precisely for that reason, the applicable discipline is the balancing of rights under Article 52(1): a limitation must be provided for by law, respect the essence of the rights concerned, and be both necessary and proportionate to the objective pursued. Proportionality is not satisfied by the importance of the objective alone. It requires that the measure be suitable, that it demonstrably delivers an actual benefit to that objective, that no less intrusive measure would achieve it, and that the benefit obtained is not outweighed by the severity of the interference.[5] A fundamental right may not be curtailed in exchange for a benefit that is asserted rather than demonstrated. No such demonstration has been made here: the European Data Protection Board and the European Data Protection Supervisor, examining the permanent proposal, concluded jointly that it does not satisfy the requirements of strict necessity, effectiveness and proportionality, and that under it the interference with the confidentiality of communications "may in fact become the rule rather than remain the exception".[6]

Generalised scanning also inverts the presumption of innocence protected by Article 48(1) of the Charter. It treats the private correspondence of every user of a service as a permissible object of inspection in the absence of any suspicion, individualised or otherwise, that the relationship between citizen and investigative measure that the presumption exists to prevent. The jurisprudence of both European courts points the same way. The Court of Justice has consistently held that general and indiscriminate measures affecting the communications of persons for whom there is no evidence of a link to serious crime exceed the limits of the strictly necessary, the very ground on which it invalidated the Data

[4]Judgment of 29 October 1980, Roquette Frères v Council, Case 138/79 [1980] ECR 3333 ("Isoglucose"), annulling Council Regulation (EEC) No 1293/79, adopted without awaiting the Parliament's opinion, for infringement of an essential procedural requirement: consultation of the Parliament allows it to play an actual part in the legislative process and is not satisfied by a mere request for an opinion.

[5]On the structure of the proportionality assessment under Article 52(1) of the Charter, suitability of the measure for attaining the objective, necessity in the sense that no less restrictive measure would suffice, and proportionality in the narrow sense, see the settled case law of the Court of Justice, including judgment of 9 November 2010, Volker und Markus Schecke and Eifert, Joined Cases C-92/09 and C-93/09, EU:C:2010:662, paragraph 74, and Digital Rights Ireland (cited in footnote 7), paragraph 46; and EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019.

[6]EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, adopted 28 July 2022, p. 12, paragraph 18.

Retention Directive, an EU-wide, suspicionless measure likewise justified by the fight against serious crime.[7] The European Court of Human Rights, in Podchasov v. Russia, held that a legal framework requiring providers to weaken end-to-end encryption, there at the demand of the Russian security services, affects all users indiscriminately, cannot be regarded as necessary in a democratic society, and impairs the very essence of the right to respect for private life.[8] Voluntary, suspicionless scanning of the private correspondence of all users of a service sits uneasily with both lines of jurisprudence: the interference is generalised, while the safeguards, judicial authorisation, prior suspicion, effective remedy, are absent.

The national constitutional record reinforces the European one. Before the Court of Justice ruled, the constitutional courts of Romania (2009), Germany (2010) and the Czech Republic (2011) had each annulled their national implementations of the Data Retention Directive as incompatible with constitutional guarantees of the confidentiality of communications, in Germany on complaints brought by some 35,000 citizens, the largest mass constitutional proceeding in German history, and when Romania legislated again, its Constitutional Court struck the replacement down as well.[9] History also shows how such measures fall. Suspicionless surveillance regimes in Europe have been ended at second reading by an assembled Parliament, annulled by national constitutional courts, invalidated by the Court of Justice on references from national courts under Article 267 TFEU[10], and condemned in Strasbourg. Each of those routes remains open against the reinstated derogation and against any permanent regime built on the same premise.

A measure of this kind does not achieve legal certainty by entering into force; it achieves a decade of litigation, at the end of which the case law has never yet vindicated the generalised, suspicionless scanning of the content of communications. Legislating against that record is a disservice to the very providers and authorities the measure is meant to empower, and to the children whose protection is made to depend on an instrument with a documented life expectancy.

[7]Judgment of 8 April 2014, Digital Rights Ireland, Joined Cases C-293/12 and C-594/12, EU:C:2014:238, invalidating Directive 2006/24/EC (the Data Retention Directive) for exceeding the limits imposed by the principle of proportionality under Articles 7, 8 and 52(1) of the Charter; judgment of 6 October 2020, La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18 and C-520/18.

[8]Podchasov v. Russia, European Court of Human Rights, judgment of 13 February 2024, holding that a statutory obligation enabling the authorities to weaken end-to-end encryption for all users cannot be regarded as necessary in a democratic society and violates Article 8 ECHR.

[9]Romanian Constitutional Court, Decision No 1258 of 8 October 2009; German Federal Constitutional Court, judgment of 2 March 2010, 1 BvR 256/08 (BVerfGE 125, 260), on constitutional complaints brought by approximately 35,000 citizens, the largest mass complaint proceeding in German history; Czech Constitutional Court, judgment of 22 March 2011, Pl. ÚS 24/10. The Romanian Constitutional Court annulled the replacement statute (Law 82/2012) on 8 July 2014. Courts in Bulgaria and Cyprus reached comparable conclusions on their national regimes.

[10]The references in Digital Rights Ireland were made by the High Court of Ireland and the Austrian Verfassungsgerichtshof, illustrating the route by which national proceedings place the validity of an EU act before the Court of Justice under Article 267 TFEU.

3. Technical reality and error at scale

Detection technologies applied indiscriminately across billions of messages produce false positives whose absolute number is large even where the error rate is small, exposing intimate lawful communications, including those of minors themselves, to review by providers and authorities. The scale is documented: according to the German Federal Government's answer to a parliamentary question, of the 91,242 reports forwarded by the U.S. clearinghouse NCMEC to the Federal Criminal Police Office between January and May 2026, approximately 40% were assessed as not criminally relevant.[11] The permanent proposal, as it stood in earlier Council negotiations, extended the debate to end-to-end encrypted services; the amended interim regime now excludes them, and the negotiators on the permanent Regulation are reported to have reached agreement on the protection of encryption, leaving the design of detection, targeted or generalised, voluntary or mandatory, as the decisive open question. Client-side scanning, the principal technique contemplated whenever encrypted services are brought into scope, requires inspecting content before encryption; the leading peer-reviewed assessment of the technique, authored by fourteen of the field's most eminent cryptographers, found no design space in which it provides substantial benefits to law enforcement without seriously risking the privacy and security of all users, and concluded that it neither guarantees efficacious crime prevention nor prevents surveillance.[12]

This is not a theoretical objection. Apple, having built such a system, abandoned it after extensive consultation, on the stated ground that it was not practically possible to implement without imperilling the security and privacy of its users and that scanning for one type of content opens the door to bulk surveillance of others.[13] **A scanning capability created for one purpose is a scanning capability available for others.**

Nor does the operational record support the premise that volume of detection translates into protection of children. The most detailed independent study of the reporting pipeline into which scanning feeds found that law enforcement is overwhelmed by the volume of reports and structurally unable to triage them or to tell which of two reports conceals ongoing abuse,

[11]Answer of the German Federal Government to a parliamentary question, published by the Bundestag in July 2026 (full text documented by netzpolitik.org, 22 June 2026, updated 16 July 2026): of 91,242 reports forwarded by the National Center for Missing & Exploited Children (NCMEC) to the Federal Criminal Police Office (BKA) between January and May 2026, the criminal-relevance rate was approximately 60 per cent.

[12]H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague and C. Troncoso, "Bugs in our pockets: the risks of client-side scanning", Journal of Cybersecurity, Vol. 10, Issue 1 (2024), tyad020, doi:10.1093/cybsec/tyad020, finding no design space for solutions that provide substantial benefits to law enforcement without seriously risking the privacy and security of all users.

[13]Apple Inc., response to the Heat Initiative, August 2023 (reported by Wired, September 2023): Apple abandoned its client-side CSAM detection project after extensive consultation, on the ground that it was not practically possible to implement without imperilling the security and privacy of users, and that scanning for one type of content "opens the door for bulk surveillance".

so that indiscriminate scanning adds volume precisely where the constraint is prioritisation.[14] Comparative experience points the same way: the official audit of the principal United States platform-liability statute adopted in the name of combating online sexual exploitation found, three years on, a single prosecution under it and enforcement continuing under pre-existing law.[15] The Commission's sole implementation report on the interim regime, published in December 2023, asserts its effectiveness, yet does so on the basis of the providers' own submissions, in reporting formats that the Parliament's responsible committee found were not standardised and not comparable across providers, and without the assessment of outcomes against existing and less intrusive measures that the EDPB and EDPS had identified as the missing precondition of any proportionality finding.[16] A conclusion of effectiveness built on the regulated entities' self-reporting, in a form that precludes comparison, is not the demonstration that Article 52(1) of the Charter requires. The co-legislators themselves now acknowledge the problem: the Council Presidency's September 2026 state-of-play note on the negotiations records that under the present voluntary regime "a high volume of reports generated do not lead to any operational outcome".[17]

4. What is at stake beyond this file

Confidential communication is not a niche interest. It is the working condition of journalism and the protection of sources, of legal professional privilege, of medical confidentiality, of the safety of victims of abuse seeking help, and of the ordinary private life of every citizen, including the children the measure is intended to protect. It is also infrastructure: commerce, public administration, and the digital economy, from banking to the digital asset sector in which many of the signatories work, rest on the dependability of encryption. A legal order in which the integrity of encrypted channels is negotiable places all of this at risk at once. The question before the co-legislators is therefore not a sectoral one; it is whether the confidentiality of correspondence remains a right in the European Union or becomes a concession.

---

[14]S. Grossman, R. Pfefferkorn, D. Thiel, S. Shah, R. DiResta, J. Perrino, E. Cryst, A. Stamos and J. Hancock, The Strengths and Weaknesses of the Online Child Safety Ecosystem, Stanford Internet Observatory (April 2024), doi:10.25740/pr592kc5483, finding that law enforcement is overwhelmed by report volume and unable to triage reports to identify children in harm.

[15]U.S. Government Accountability Office, Sex Trafficking: Online Platforms and Federal Prosecutions, GAO-21-385 (June 2021), finding that as of March 2021 the FOSTA statute had been used in a single federal prosecution and that no restitution had been sought or awarded, while enforcement continued under pre-existing statutes.

[16]European Commission, Report on the implementation of Regulation (EU) 2021/1232, COM(2023) 797 final, 19 December 2023, concluding on the basis of reports submitted by the providers that the interim regime appears effective. Cf. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report A9-0021/2024, noting that in the absence of a reporting template under Regulation (EU) 2021/1232 providers shared different types of information which were not necessarily comparable; and EDPB-EDPS Joint Opinion 4/2022, paragraphs 42–46, on the absence of an assessment of the effectiveness of existing measures.

[17]Council of the European Union, Presidency note 11956/26 of 10 September 2026, "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – State of play and way forward" (LIMITE; reported in the press), point (iii).

IV. Proposals

Each proposal below states its mechanism. This statement does not ask the legislator for guidance; it proposes the content of a framework that would protect children effectively while respecting the Charter.

1. Targeted detection orders in place of generalised scanning.

Detection should be permissible only pursuant to an order issued by a judicial authority, directed at identified users or accounts in respect of whom objective evidence gives rise to suspicion, limited in time, and subject to renewal only on fresh judicial review. This preserves an effective investigative tool while restoring the link between interference and suspicion that Article 52(1) of the Charter requires. Safeguards must foreclose function creep: orders strictly limited to the investigation for which they are issued; no order on the basis of an anonymous denunciation alone, absent corroborating objective evidence; notification of the person concerned once the investigation permits, with an effective remedy; and public statistics on orders sought, granted, and refused. Authorisation must remain individualised: a judicial or administrative authorisation of a provider's "search plan" covering the communications of all users for a period of time is generalised scanning under another name, and the involvement of an authority does not cure what Article 52(1) forbids. Mechanism: detection orders in the permanent Regulation issued ex ante by a judicial authority under the conditions and safeguards above, replacing all provisions for generalised detection. The Parliament's negotiating position on the permanent Regulation has pointed in this direction; the autumn negotiations should adopt it.

2. Less intrusive signals before content inspection.

Where providers act protectively, behavioural indicators offer a considerably narrower interference than the analysis of message content: mass contact requests directed at minors, rapid account recreation after blocking, repeated blocks or reports, age-disparate contact patterns, and movement between many child accounts. Behavioural metadata can still be intrusive and requires its own safeguards, yet it permits protective intervention without reading anyone's correspondence. Mechanism: recognition in the permanent Regulation of behavioural-signal analysis, subject to data-protection safeguards, as the first-line protective measure, with content inspection reserved for targeted judicial orders.

3. An EU Centre focused on removal at source.

The proposed EU Centre should be mandated and resourced to pursue the systematic identification and removal of known abuse material from publicly accessible services, where the material demonstrably circulates, rather than the inspection of private correspondence. Mechanism: a statutory notice-and-takedown authority with binding deadlines; hash-database stewardship under EDPB oversight, with judicial validation of database entries and human verification before removal decisions; fast cross-border removal and victim-notification procedures; and annual public reporting of removal outcomes.

4. Safety by design, not surveillance by default.

Services accessible to minors should carry design obligations that do not presuppose identifying every user: default-private profiles for minors, restrictions on unsolicited contact from unknown adults, limits on unsolicited media, warnings before the sharing of intimate images, controls over discoverability, and auditable age-appropriate design codes, enforced through the existing Digital Services Act supervisory architecture rather than a parallel scanning regime. Nothing in this proposal should be read as a call for mandatory age verification. Age-assurance regimes as deployed today compel generalised identity disclosure and the mass collection of sensitive data, replicating the very harms this statement opposes, as recent national experience with mandatory age verification has demonstrated. The proportionate path is different: the co-legislators should create recognition and acceptance pathways for privacy-preserving age-assurance technologies, including zero-knowledge attestations that prove an attribute such as age without revealing identity, so that protection of minors can be strengthened as these tools mature, without building new data-collection obligations. Mechanism: a mandate to the Commission, supported by the European standardisation bodies, to define baseline technical requirements for privacy-preserving age assurance, with regulatory acceptance conditional on data minimisation by design.

5. **A statutory protection for end-to-end encryption.**

The amended interim regime now excludes end-to-end encrypted communications from its scope, an exclusion Parliament secured at second reading. The permanent Regulation should entrench the same protection as an operative provision, stating expressly that no obligation it creates may be construed to require a provider to weaken, circumvent, or create access to end-to-end encryption, including by client-side scanning. Mechanism: an operative article, not a recital, mirroring the technique used elsewhere in the acquis where the co-legislators have wished to place a technology beyond the reach of implementing measures.

6. **Transparency obligations for the interim period.**

For so long as the reinstated derogation operates, providers making use of it should report annually, to the supervisory authorities and publicly: the technologies deployed; the volume of communications scanned; the number of reports made and the number of duplicate reports; the proportion of reports subsequently assessed as unfounded; and the outcomes obtained, including victims identified and rescued, prosecutions commenced, and material removed. Where private communications are scanned, the processing should leave an auditable record, accessible to the supervisory authority and, once disclosure can no longer prejudice an investigation, to the user concerned. Mechanism: annual public reporting by providers is already required by Article 3(1), point (g)(vii), of Regulation (EU) 2021/1232; the co-legislators should render it granular, mandatory in the elements above, standardised through a common reporting template, and consolidated by the Commission in a single annual publication, so that the autumn negotiation proceeds on evidence rather than assertion.

7. **A procedural safeguard for resubmitted texts.**

Where a text substantively identical to one Parliament has rejected within the same term is resubmitted, the request for urgent procedure should require referral to the committee responsible before any plenary vote. The events of July show the need: the urgent procedure bypassed committee scrutiny, and only the chamber's ability to assemble an amending majority prevented the unamended text from entering into force over the objection of a majority of those voting. Mechanism: an amendment to Parliament's Rules of Procedure, which lies within Parliament's own competence and requires no Treaty change.

V. Engagement

What is defended in this statement is not an industry position. It is the proposition that fundamental rights are limited only where a demonstrated benefit justifies it, through targeted means, under judicial control. We welcome the opportunity to discuss these proposals with the negotiating teams, shadow rapporteurs, Member State representatives and the Commission services ahead of and during the autumn negotiations, including through short briefings on how the proposed measures work in practice. Practitioners behind this statement, including engineers working on privacy-preserving protection technologies, are available for that purpose.

Contact: Mariana de la Roche Wills, BlackVogel Consulting — info@blackvogel.com

Expert contributions

This statement benefited from the contributions of experts in law, compliance, cryptography, child protection and policy. Contributors are named exclusively with their express consent; further contributions were received from experts who prefer to remain unnamed.

Mariana de la Roche (BlackVogel, DAAvern), Kamilla Szocs (BlackVogel), Karola Xenia Kassai (KassaiLaw), Rebeca Dos Reis (BlackVogel), Raido Saar (ComplyOnce), Tommaso Astazi (Blockchain for Europe).

With the support of:

Juan Ignacio Ibañez (MiCA Crypto Alliance), Mauricio Magaldi (Venture Builder, IOG; BlockDrops), Seth Hertlein (Ledger)