sciendo

Identity verification in virtual shareholders' meetings: normative foundations and legal consequences

Andres Vutt
Margit Vutt
Maris Vutt

School of Law
University of Tartu
Näituse 20
Tartu 50409, Estonia
andres.vutt@ut.ee
margit.vutt@ut.ee
maris.vutt@ut.ee

Abstract: The digital transformation of corporate governance has rendered virtual shareholders' meetings a permanent feature of modern company law. While electronic participation enhances accessibility and cross-border engagement, it raises fundamental questions concerning the reliable identification of participants. This article examines identity verification in virtual shareholders' meetings of private limited companies under Estonian law, with comparative references to German law.

The analysis is based on the understanding that identity verification is not a mere technical formality but constitutes a structural precondition for the lawful formation of the company's collective will. Although Estonian law permits electronic participation by default, it does not prescribe any specific authentication standards. The legal requirement that only shareholders or duly authorised representatives may exercise membership rights therefore remains unchanged, while the technical means used to ensure compliance vary.

The article adopts a functional perspective on identity verification. It examines different forms of authentication that may be used in virtual meetings, including the Estonian state e-identity, other digital identification means (such as those recognised under the eIDAS framework), as well as situations where no formal digital

https://doi.org/10.2478/bjes-2026-0015 *TalTech Journal of European Studies*, 16(2(45))
Tallinn University of Technology (ISSN 2674-4619)

identification is available. The discussion highlights how varying degrees of technical reliability may influence legal certainty and the protection of participation rights.

Particular attention is given to the legal consequences of defective identification. Drawing on Estonian case law concerning digital signatures, the article analyses the presumption arising from the use of electronic identification tools, the formal requirements of representation, and the distinction between void votes and the revocation or nullity of resolutions. It argues that identity verification serves a procedural legitimising function and does not replace the substantive determination of share ownership. Virtual meetings therefore require not the creation of new legal principles but a careful functional adaptation of established company-law concepts to a technologically mediated environment.

Keywords: *electronic participation, Estonian company law, identity verification, shareholder identification, validity of resolutions, validity of votes, virtual shareholders' meetings*

1. Introduction

The rapid digitalisation of corporate governance has fundamentally transformed the way shareholders exercise their membership rights. While remote participation in general meetings had been gradually developing for more than a decade at the European level, particularly following the adoption of the Shareholder Rights Directive, the COVID-19 pandemic acted as a catalyst, accelerating the widespread introduction of fully virtual or hybrid meetings across jurisdictions. Digital shareholder meetings are no longer a marginal phenomenon but have become an established governance tool both globally and within the European Union. Their practical advantages are evident: they facilitate cross-border participation, reduce organisational costs, and increase accessibility for dispersed shareholders. At the same time, they challenge traditional assumptions underlying company law, which has historically been shaped by the paradigm of the physically convened meeting.

A particularly delicate and structurally important issue relates to ensuring the proper identification of meeting participants. At traditional in-person meetings, identification is secured through layered safeguards: physical attendance, presentation of identification documents, familiarity among

participants, and reference to shareholder registers or attendance records. In the context of virtual meetings, however, these safeguards are either absent or replaced by technologically mediated processes. Identity verification therefore becomes dependent on electronic authentication tools, platform architecture, and data-processing solutions, often developed by private service providers whose primary objective is communication efficiency rather than legal certainty. This shift exposes a range of doctrinal and practical problems: the absence of uniform statutory standards; the risk of unauthorised participation or misuse of access credentials; the verification of representatives and the validity of powers of attorney; and the interplay between authentication mechanisms and data protection requirements under EU law. Ultimately, defective identification may affect not only the validity of individual votes but also the legal status of resolutions adopted at the meeting.

In Estonia, the legal basis for digital participation in meetings of legal persons was introduced in May 2020. The new regulation (*Act on the General Part of the Civil Code (Estonia) 2002*, Section 33[1]) enabled shareholders, as well as members of a body of every other legal person, to participate in a meeting through real-time two-way communication or by other similar electronic means that enable the member, while being at a remote location, to follow the meeting, speak, and vote when resolutions are adopted. Although the statutory wording frames electronic participation as an individual right of the shareholder, legal scholarship has interpreted this provision more broadly as constituting the general legal basis for the convening and conduct of virtual meetings (Vutt and Vutt, 2021, p. 445; Vutt, 2024, p. 12). Importantly, the Estonian model is structured as an opt-out system: unless the law or the articles of association provide otherwise, electronic participation is permissible by default. The provision does not, however, prescribe specific technical standards for identity verification. It determines the admissibility of the meeting format but leaves the concrete authentication mechanisms largely to the autonomy of the company. As a result, the legal requirement that only shareholders or their duly authorised representatives may participate remains unchanged, whereas the tools used to ensure compliance with that requirement vary considerably in practice.

The digital transformation of corporate governance has rendered virtual shareholders' meetings a permanent feature of modern company law. While electronic participation enhances accessibility and cross-border engagement, it raises fundamental questions concerning the reliable identification of participants. This article examines identity verification in

virtual shareholders' meetings of private limited companies under Estonian law, with comparative references to German law.

The analysis is based on the understanding that identity verification is not a mere technical formality but a structural precondition for the lawful formation of the company's collective will. Although Estonian law permits electronic participation by default (*Act on the General Part of the Civil Code (Estonia) 2002*, Section 33[1]), it does not prescribe specific authentication standards. The legal requirement that only shareholders or duly authorised representatives may exercise membership rights therefore remains unchanged, while the technical means of compliance vary.

The article adopts a functional perspective on identity verification. It examines different forms of authentication that may be used in virtual meetings, including the Estonian state e-identity, other digital identification means (such as those recognised under the eIDAS framework), as well as situations where no formal digital identification is available. The discussion highlights how varying degrees of technical reliability may influence legal certainty and the protection of participation rights.

Particular attention is devoted to the legal consequences of defective identification. Drawing on Estonian case law concerning digital signatures, the article analyses the presumption arising from the use of electronic identification tools, the formal requirements of representation, and the distinction between void votes and the revocation or nullity of resolutions. It argues that identity verification serves a procedural legitimising function and does not replace the substantive determination of share ownership. Virtual meetings therefore require not new principles, but a careful functional adaptation of established company-law concepts to a technologically mediated environment.

Against this background, the present article examines the verification of shareholder identity in virtual meetings of private limited companies (*osaühing*) under Estonian law, in comparison with German law relating to the *GmbH* and, where relevant, stock corporation law. The article seeks to answer the question: What is the normative foundation of the requirement to verify the identity of participants in shareholders' meetings, how does it apply in a virtual environment, and how should different authentication scenarios (use of state-issued e-identity, other digital identification means, or the absence of digital identification) be assessed from the perspective of legal certainty and shareholder protection? The article further examines the

legal consequences of defective identification for the validity of votes and resolutions, and considers how the allocation of risks and burdens of proof should be structured.

By addressing these questions, the article seeks to outline a structured approach to identity verification in digital shareholders' meetings that safeguards the integrity of the decision-making process while taking into account technological neutrality and corporate autonomy. Through a comparative analysis of Estonian and German law, focusing on private limited companies, the study examines how traditional company-law concepts may be applied and, where necessary, adapted to the digital environment without undermining the core principles of membership rights and collective will-formation.

2. Identity verification as a general precondition for shareholders' meetings

The identification of participants at a meeting is one of the central prerequisites for the lawful conduct of a shareholders' meeting. Participation in a shareholders' meeting entails more than mere physical presence. The meeting serves as the forum in which the shareholders' collective will is formed (Fleischer and Goette, 2026, § 48 Rn. 12). Accordingly, the right to participate inherently encompasses the right to take part in the process of will-formation.

The exercise of shareholder rights—particularly the right to vote, the right to speak, and the right to submit questions—presupposes that those rights may be exercised only by persons who are legally entitled to do so or acting on the basis of a valid representative relationship. This constitutes a fundamental principle governing the conduct of meetings that applies irrespective of the technical means by which the meeting is held.

Estonian law does not contain explicit provisions requiring the identification of participants in a meeting; however, this obligation arises indirectly from the requirement to draw up a list of meeting participants. Specifically, Section 171(4) of the *Commercial Code (Estonia) 1995* provides that a list of shareholders attending the meeting shall be prepared, indicating each participant's name, the number of votes attached to their shares, and the manner in which they participate in the meeting, as well as the names of

their representatives. The list must be signed by the chair of the meeting and the recorder, as well as by any shareholder or representative who is physically present at the meeting.

At traditional in-person meetings, the verification of participants' identities typically occurs through a combination of formal and informal mechanisms. These may include participant registration and the presentation of identity documents, personal identification by the management board or other attendees, and reliance on the shareholder register. Although such mechanisms are generally not regulated in detail by law, in practice they function as an implicitly assumed and socially established safeguard that links the physically present individual to their status as a shareholder or confirms their authority to act as a representative.

In the German *Act on Limited Liability Companies 1892*, unlike in stock corporation law under *Stock Corporation Act (Germany) 1965*, § 129(1), there is no statutory provision requiring a formal determination of the persons present at a shareholders' meeting. However, an obligation to establish attendance may arise from the company's articles of association, especially where they regulate the procedure of the shareholders' meeting in more detail (Noack, 2025, § 28, Rn. 26). If the articles require that minutes be prepared for every shareholders' meeting, this generally includes the preparation of an attendance list as a necessary component of the minutes (Fleischer and Goette, 2026, § 48 Rn. 132; Altmeppen, 2023, § 48 Rn. 32–35).

It has been pointed out that even in the absence of a specific legal or statutory duty, establishing attendance is considered to be advisable in practice (Noack, 2025, § 28 Rn. 27). It facilitates verification of the quorum and may also help rebut objections concerning the validity of resolutions, for example in case all the shareholders are present (*Act on Limited Liability Companies (Germany) 1892*, § 51(3)). In practice, two main methods of determining attendance can be observed. Where a chairperson of the meeting has been appointed, the chair will typically establish attendance at the beginning of the meeting; this is generally regarded as part of the chair's duties even without an explicit provision in the articles (Noack, 2025, § 28 Rn. 40–41; Wicke, 2024, Rn. 3; Lange, 2015, p. 179). If no chair has been appointed, attendance is often recorded either by means of a list at the entrance to the meeting venue or through a circulation procedure (Michalski *et al*., 2023; *Act on Limited Liability Companies (Germany) 1892*, § 48 Rn. 129–130).

One may conclude that the identification of participants is not a mere technical formality but a structural precondition for the lawful formation of the company's collective will. The exercise of core membership rights—

especially voting, speaking, and asking questions—requires that only persons entitled by law or through valid representation be admitted. Even in the absence of explicit statutory provisions, this obligation arises implicitly from procedural requirements such as the preparation of attendance lists and the verification of quorum. Estonian and German law show that identification mechanisms, whether statutory, statutory-based, or practice-based, serve to link participation to shareholding status while preventing the meeting from becoming a forum for resolving substantive ownership disputes. This functional approach, applicable to both physical and virtual meetings, underscores that reliable identification is indispensable for the validity and integrity of shareholders' resolutions.

3. Specific issues of identity verification at virtual shareholders' meetings

The legal framework governing the identification of shareholders in both physical and virtual general meetings is, in principle, comparable under Estonian and German law. At the EU level, the legislative development of remote participation has been shaped primarily by the Shareholder Rights Directive, in force since 2007 ('Council directive 2007/36/EC', 2007). Article 8 of the Council directive requires Member States to permit companies to offer shareholders participation in general meetings by electronic means, such as real-time transmission of the meeting or real-time two-way communication enabling shareholders to address the meeting from a remote location. Article 8(2) further provides that the use of electronic means for participation may be made subject only to such requirements and constraints that are necessary to ensure the identification of shareholders and the security of electronic communication, and only insofar as these requirements are proportionate to those objectives.

It should be noted, however, that the Directive was designed to harmonise only the legislation of Member States concerning listed companies. More detailed rules on the identification of shareholders participating electronically were therefore left outside the scope of harmonisation. Consequently, neither the Estonian nor the German legislature introduced specific statutory provisions on this matter when implementing the Council directive.

In Estonia, no rules on virtual meetings existed for private limited companies until May 20, 2020, when the *Act on the General Part of the Civil Code*

was amended to introduce a general provision permitting all types of legal entities to hold meetings by electronic means (Vutt, 2020, p. 37). Even under the current legal framework, the determination of the precise technical requirements for conducting virtual meetings remains largely within the autonomy of the company.

In August 2022, the Informal Company Law Expert Group (ICLEG) published a report on virtual shareholder meetings in which the experts observed that Member States' practices regarding shareholder identification vary considerably. They concluded that this issue would be difficult to regulate in much greater detail than by requiring companies to adopt appropriate, non-discriminatory measures to identify their shareholders. The report further noted that, in many jurisdictions, companies identify shareholders in practice through individual access codes sent to them, often administered by specialised service providers. In other jurisdictions, comparable authentication mechanisms are used, frequently based on two-factor authentication. Strictly speaking, such mechanisms do not amount to identification in the formal sense, as they merely establish that the participant is in possession of the access credentials transmitted by the company to the shareholder's address.

In German legal literature, it has been argued with regard to the identification of participants in a virtual general meeting that the law does not lay down any specific requirements as to the level of identification. It follows from the statutory framework that identification is sufficient if shareholders are connected to the meeting in a manner that enables them to exercise their participation rights. Accordingly, a company may, in principle, limit itself to entering into the list of participants the person whose access credentials were used to log in to the meeting (Walch and Häuslmeier, 2023, p. 121). Although pragmatic in nature, this solution may fall short of providing the degree of legal certainty required.

If shareholders do not attend the meeting in person, several identification mechanisms inherent in physical meetings are excluded, and identity verification inevitably becomes a technologically mediated process (Zetzsche *et al.*, 2021, p. 28). A person's presence can no longer be inferred from their location in a specific physical space but must instead be established through technological means. Consequently, in the context of virtual meetings, identity verification as such becomes more visible and more sensitive, even though its substantive purpose remains unchanged. Hence, although virtual meetings offer numerous advantages, they also entail significant risks,

particularly with regard to the reliable verification of participants' identities and the technical vulnerabilities inherent in such systems (Romashchenko and Bitė, 2024, p. 2).

From a doctrinal perspective, however, the virtual format of a meeting does not alter the objective of identity verification, which continues to be the safeguarding of the integrity of the company's decision-making process and the equal treatment of shareholders. Accordingly, the requirements for identity verification cannot be fundamentally different merely because the meeting is conducted by electronic means. What changes is not the legal requirement itself, but the means by which it is fulfilled.

Identity verification must therefore be understood as a functional requirement: the measures applied must be suitable and sufficient to reliably link participation in the meeting to the respective person's status as a shareholder or to a valid power of representation. Such a functional approach provides a conceptual basis for assessing virtual authentication solutions within the framework of existing company law, including Estonian law, without presupposing any fundamental distinction between physical and virtual shareholder meetings.

Although the requirement of identity verification is identical in both physical and digital meetings, the virtual format gives rise to a number of specific situations that either do not occur in physical meetings or arise to a significantly lesser extent. These challenges stem primarily from the use of a digital communication environment and the absence of direct interpersonal contact.

The first issue concerns the lack of clear and uniform legal standards. Company law formulates the right to participate in abstract terms, requiring that only shareholders or their duly authorised representatives attend the meeting, but it does not prescribe specific mechanisms for identity verification in a virtual environment. In other words, the law determines the required outcome, but not the means by which it is to be achieved. Such an approach is, in itself, justified, since overly detailed regulation would effectively require the legislature to prescribe specific technical solutions for companies. Moreover, excessively precise rules could undermine technological neutrality (Jerzmanowski, 2020; Ruiu, Saiu and Grosso, 2024, p. 7), as the legislature would need to take into account all existing and potentially future technological options—an undertaking that is clearly impossible. Regulatory indeterminacy may, however, lead to the development of fundamentally divergent practices. Taken alone, this is

not necessarily problematic, at least insofar as the objectives of identity verification are achieved. As noted above, the law prescribes the outcome, while each company remains free to choose the means to attain it.

It must also be recognised that different practical constellations emerge in the identification of meeting participants. In a company whose shareholders all know one another personally, incorrect identification is practically inconceivable. By contrast, in a company with several hundred shareholders—particularly where shares are freely transferable—it is unrealistic to assume that the chair of the meeting could even know every participant personally, even in theory.

A second significant issue concerns reliance on existing technological solutions, which are typically developed by private service providers and are not specifically designed to meet the requirements arising from company law. The primary function of online meeting platforms is to facilitate communication, not to ensure legally reliable identity verification. Usernames, passwords, or meeting links may restrict access, but they do not necessarily establish a sufficiently secure link between the participant and their status as a shareholder or representative.

Besides MS Teams and dedicated electronic meeting environments, companies in various jurisdictions also use widely available platforms such as Zoom and Google Meet (Vutt, 2024, p. 45). Standard applications offer convenience and familiarity, as many users are already accustomed to them, whereas specialised platforms may require additional adaptation. Specialised solutions, however, can provide tailored functionalities, including attendance monitoring, identity verification, recording, and automated summaries, and may be designed to meet a company's specific needs. This customisation can be advantageous, particularly for larger companies, but it may also entail higher costs and prove disproportionate for companies with only a small number of shareholders (Romashchenko, 2026, p. 2).

Accordingly, the use of standard applications is understandable in practice. Nevertheless, companies relying on such tools must ensure that the requirements of participant verification are not compromised and that the identities of all attendees are properly verified.

Thirdly, in virtual meetings, the risk of unauthorised participation and identity misuse increases. Access credentials may be shared with third parties, user accounts may be used by multiple individuals, or an individual may act under a false identity, often without immediate detection. Such risks

directly affect the legitimacy of resolutions made at shareholder meetings and may give rise to disputes over their validity.

The situation becomes even more complex when a shareholder participates through a representative. Estonian law imposes no restrictions on who may act as a representative. Section 170(3) of the *Commercial Code (Estonia) 1995* only requires that the existence of the authority granted to the representative must be evidenced by a document in a form capable of being reproduced in writing. If a representative participates, it is necessary to verify not only that person's identity but also the existence, validity, and scope of the authorisation. The situation is simplified if the shareholder has signed the power of attorney with a recognised digital signature, such as the national digital signature available in Estonia. However, the company cannot mandate this form of signing, since doing so would effectively prevent shareholders who lack access to such a digital signature from exercising their right to participate through a representative.

Finally, identity verification in virtual meetings is closely intertwined with issues of personal data protection. Effective authentication mechanisms often require the processing of personal data, including identification data or electronic identity credentials. In doing so, the company must ensure that the processing of personal data complies with data protection principles, in particular the principles of purpose limitation and data minimisation laid down in Article 5 of the General Data Protection Regulation (GDPR), while at the same time maintaining a sufficient level of reliability.

A virtual general meeting may involve the processing of types of personal data that differ from, or extend beyond, those processed during a meeting held in physical presence. In particular, this typically includes the participant's IP address and login credentials, such as a username and access code required to access the virtual meeting platform. Where the technical setup allows participants to actively engage—for example, via two-way audio or video communication—image and voice data may also be processed. Furthermore, any third-party service providers assisting with the organisation or technical operation of the virtual meeting must be properly integrated in accordance with applicable data protection laws (notably with respect to processing on behalf of the controller), and appropriate technical and organisational measures must be implemented to ensure an adequate level of protection of participants' personal data. However, these requirements are not unique to virtual general meetings; they reflect general data protection obligations that apply regardless of the format in which the meeting is held (Apel and Nägele, 2025, Rn. 2).

One instrument that companies might consider using for the identification of their shareholders is facial recognition technology. However, its use gives rise to significant legal concerns, rendering this method of identification highly questionable. Under the GDPR, the concept of personal data is construed broadly and encompasses biometric information. As a rule, the processing of biometric data for the purpose of uniquely identifying a natural person is prohibited, unless a specific legal basis applies, most notably the explicit consent of the data subject. Biometric data is generated where a person's physical, physiological, or behavioural characteristics are measured and used for identification purposes. Accordingly, if a company employs facial recognition technology to verify shareholders electronically and thereby generates biometric templates, it will, in most cases, be required to obtain the explicit consent of the individuals concerned (Romashchenko, 2026, p. 14).

It should also be borne in mind that electronic shareholder identification relying on AI-based biometric systems falls within the scope of the EU's existing regulatory framework on artificial intelligence, namely the AI Act. Annex III (1(a)) lists remote biometric identification systems, including facial recognition systems, as high-risk AI systems. Consequently, pursuant to Article 113 as of August 2, 2026, such forms of remote biometric identification are classified as high-risk AI systems.

Considered cumulatively, these challenges illustrate that virtual shareholder meetings cannot be regarded as a mere technical transposition of their physical counterparts. Rather, they expose structural questions concerning the verification of participants' identities, thereby necessitating a critical re-examination of established legal assumptions and the development of functionally equivalent authentication mechanisms specifically tailored to the digital environment.

4. Identity verification at virtual shareholders' meetings under Estonian law

In the Estonian legal system, the issue of identity verification at virtual shareholders' meetings must primarily be addressed by distinguishing whether the participant is able to use an Estonian state-issued electronic identification (e-ID) means. This distinction makes it possible to structure the analysis according to the technical reliability of the authentication method and its legal significance.

4.1 Identity verification using the Estonian state e-identity

Where a shareholder or their representative uses an Estonian state-issued electronic identification (e-ID) to participate in a virtual shareholders' meeting, the verification mechanism can achieve a particularly high degree of technical and legal reliability. In such cases, authentication does not merely serve as a means of controlling access to the online meeting environment but also entails active confirmation of the participant's identity.

One possible solution is to require participants to log into the virtual meeting platform using their state-issued e-identity. In practice, this may involve redirecting the participant, prior to the meeting or at its initial stage, to an authentication interface where they confirm their identity using an ID card, Mobile-ID, or Smart-ID. During the authentication process, the participant's identity is cryptographically verified and linked to their personal identification code.

It is also possible to send the shareholders, via the contact method and address indicated by them, a document containing a registration form that the shareholder must digitally sign and return to the chair of the meeting in order to register.

The requirements for an electronic signature are laid down in Section 80(1) of the *Act on the General Part of the Civil Code (Estonia)* 2002, according to which an electronic signature must be given in a manner that enables it to be linked to the content of the transaction, the person performing the transaction, and the time of the transaction. The rules for attributing an electronic signature to a person and for issuing such signatures are established by law. A digital signature also qualifies as an electronic signature.

At the EU level, electronic signatures are regulated by the eIDAS Regulation and, at the national level, additionally by the Estonian *Electronic Identification and Trust Services for Electronic Transactions Act* (EUTS), which establishes domestic rules for the issuance and use of certificates for electronic signatures.

It follows that, for identity to be regarded as duly verified, it is not decisive merely that the shareholder has been authenticated at a particular moment. Equally important is that the outcome of authentication is specifically linked to the shareholder's participation in the meeting. This means that the system must be capable of binding the authenticated person to a specific participant account, user session, or "seat" in the meeting, thereby preventing a situation where, following authentication, another person gains access to the meeting. Such linkage may be ensured, for example, through single sign-on or session-based authentication.

In addition, identity verification may be strengthened by requiring electronic signatures for certain actions, such as voting or submitting a proxy. Where a shareholder casts a vote or confirms their participation using a qualified electronic signature, an additional and subsequently verifiable link is established between the specific declaration of intent and the individual concerned. From a functional standpoint, such a solution is comparable to signing an attendance list at a physical meeting.

From a legal perspective, it is important that the technical solution used allows the organiser of the meeting to document the authentication process. This may include recording the time of authentication, the identification means used, and the link to the specific meeting participant. Such documentation is not required solely for technical control purposes but is also of significance in the event of subsequent disputes, where it may need to be assessed whether only authorised persons participated in the meeting.

In conclusion, the Estonian state e-identity enables identity verification at virtual shareholders' meetings in a manner that satisfies both a high standard of legal certainty and the functional logic of company law. Although the use of such solutions is not legally mandatory, it provides a clear and technically well-founded benchmark on the basis of which identity verification may be considered duly carried out.

4.2 Identity verification without the Estonian state e-identity

In situations where a shareholder or their representative does not possess an Estonian state-issued electronic identification means, alternative technical and procedural solutions must be employed to verify identity. Such situations are particularly characteristic of companies with an international shareholder base and cannot, in themselves, exclude a shareholder's right to participate. At the same time, they are associated with a lower degree of legal certainty and a greater need for supplementary safeguards.

4.2.1 Identity verification using other digital identification means

The first group of cases comprises situations in which a shareholder or their representative uses another digital identification means that is not an Estonian state e-identity. These may include electronic identities issued by other states, electronic identification means recognised under the eIDAS Regulation ('Council regulation (EU) 910/2014', 2014), as well as private-sector solutions that allow identity confirmation at a certain level.

Technically, such authentication may be carried out in a manner similar to the use of the Estonian e-identity: prior to or at the beginning of the meeting, the participant is redirected to an authentication interface where they confirm their identity using the relevant digital identity means. As a result of authentication, a link is established between the participant's digital identity and their user account or meeting session. However, the reliability of such a solution depends to a large extent on the legal recognition and technical security of the identification means used.

From a legal standpoint, the central question is whether the identification means used makes it possible, with sufficient certainty, to link the participant to a specific individual and whether it produces legally recognised effects under Estonian law. Where the identification means is mutually recognised under the eIDAS Regulation, its use may be functionally comparable to that of the Estonian state e-identity. In the case of private-sector solutions, by contrast, their reliability must be assessed separately and, where necessary, supplemented by additional control mechanisms.

In such situations, legal certainty may be enhanced through supplementary measures, such as prior submission of documents, verification of powers of attorney, or the use of electronic signatures to confirm specific actions. The weaker the legal status of the identification means used, the more important procedural and documentary safeguards become.

4.2.2 Identity verification in the absence of any digital identification means

The second group of cases consists of situations in which a shareholder or their representative lacks any digital identification means whatsoever. In such cases, cryptographically strong authentication cannot be applied, and identity verification must rely on a combination of technical and procedural measures.

In practice, this may require the shareholder to undergo a pre-registration process prior to the meeting, during which they submit a copy of an identity document and, where necessary, a power of attorney. On the basis of the submitted documents, the meeting organiser may verify the shareholder's or representative's right to participate and establish a link between the specific individual and the user account granting access to the meeting. During the virtual meeting, identity verification may be further strengthened, for example, through visual identification by comparing the participant via video with the previously submitted document.

In such solutions, the reliability of identity verification is inevitably lower than in cases involving digital identification means. There is also a greater risk of misuse of documents or unauthorised access by third parties. Consequently, the company's obligation to assess the adequacy of the measures applied becomes more significant, taking into account the importance of the meeting and the weight of the resolutions to be adopted.

From a legal perspective, the absence of a digital identification means does not in itself preclude participation in a virtual shareholders' meeting. However, achieving legal certainty in such cases requires multilayered and carefully documented solutions. The more identity verification relies on non-automated and subjective elements, the greater the risk of subsequent disputes, and the more important it becomes to establish clear internal procedural rules within the company.

5. Legal consequences of defective identity verification

Errors in the identification of shareholders may give rise to a range of legal consequences. First, such errors may be analysed from the perspective of the validity of a vote as an instrument of will-formation necessary for the adoption of corporate resolutions. Under the *Act on the General Part of the Civil Code (Estonia)* 2002, Section 33(1), the casting of a vote constitutes a legal transaction (Varul *et al*., 2023, § 33 comm. 3.5; similarly in Germany: Goette, Habersack and Kalss, 2023, § 77 Rn. 23). For a transaction to produce legal effects, it must, first, contain a declaration of intent by the person performing the transaction; such a declaration requires both an internal intention and its externally recognisable expression. Second, in order to produce legal consequences, the transaction must be valid (Varul *et al*., 2023, § 84 comm. 3.1).

At present, no Estonian case law specifically addresses digital meetings (Vutt, 2024, p. 80). The Supreme Court of Estonia has not adjudicated any such disputes, nor, to the authors' knowledge, have any such cases been addressed by the courts of first or second instance. Nevertheless, Estonian case law does contain general positions regarding the use of digital ID in the conclusion of contracts, which are, at least in part, applicable by analogy to participation in shareholders' meetings. Since the casting of a vote constitutes a declaration of intent, the legal positions developed in relation to defects in declarations of intent made in the context of contract formation are transferable to voting. Voting, in turn, presupposes the identification of the participant in the meeting. Accordingly, following the general logic of private law and taking into account both the general rules governing transactions and the positions expressed in disputes concerning the validity of resolutions and votes, it is possible to draw conclusions from the existing case law regarding defects in identification as a precondition for participation in shareholders' meetings.

Judicial protection may become necessary in situations where participation in a digital meeting is effected through the use of another individual's recognised digital identity. In this context, two distinct scenarios must be distinguished. First, a person may have voluntarily given an ID card or other authentication device to a third party. Second, the device may have left the person's possession against their will. It should be borne in mind that such identification tools are merely one means of verifying identity, and violations of this kind are therefore likely to occur relatively infrequently in

practice. They cannot, however, be excluded entirely. If, at a digital meeting, a vote is cast on behalf of a shareholder by using another person's digital ID, the legal positions developed by the courts in cases concerning contracts concluded in a similar manner become applicable.

One issue addressed by the Supreme Court in several judgements concerns the identification of persons by electronic means in contractual disputes where the central question has been whether a person may be released from the obligation to perform a contract if an ID card and PIN codes were used to conclude the contract not by them personally, but by another individual.

In civil case No. 2-16-124450 (Supreme Court of Estonia, 2019), the dispute concerned an instalment sales contract concluded through an online store. The seller brought a claim for payment against the alleged buyer on the basis that a valid contract had been concluded between them. The Supreme Court explained that where a declaration of intent aimed at concluding a contract is made in a person's name using that person's ID card and PIN codes, it must be presumed that the declaration of intent was made by the person to whom the ID card and PIN codes were issued. The burden of proof rests with the individual in whose name the declaration was made and who denies having made the declaration of intent. For example, such a person may prove that the ID card and PIN codes issued to them left their possession without fault on their part and against their will (Supreme Court of Estonia, 2019, para. 22). The Supreme Court has held that where Smart-ID codes have been obtained fraudulently, this does not amount to a voluntary transfer of the codes, and the rules on authority are therefore inapplicable (Supreme Court of Estonia, 2024, para. 11).

The Supreme Court has taken the position that if a person voluntarily gives their ID card and PIN codes into the possession of a third party, the identification tools have not left the owner's possession against the owner's will. In such a case, the provision of the ID card and PIN codes to a third party may be treated as a situation in which the owner of the ID card has granted the third party a general authorisation to conclude transactions (Supreme Court of Estonia, 2019, para. 23).

The next issue arising from the case law of the Supreme Court concerns the standard of care required in storing an ID card and PIN codes. The Supreme Court has noted that, since a digital signature has the same legal effect as a handwritten signature, the required standard of care is high. The voluntary transfer of digital-signature creation devices to a third party entails the risk that the recipient may use them beyond the specific purpose

for which they were provided and, by acting as the ID card holder, issue further declarations of intent in that capacity, in circumstances where the counterparty has no reasonable grounds to doubt that the declaration was made by the ID card holder (Supreme Court of Estonia, 2019, para. 23).

As regards the legal qualification of relationships arising from the use of another person's identification instruments, in a situation where a person voluntarily transfers all of digital-signature creation devices to a third party, who then uses them to conclude a transaction—not as a representative but by posing as the holder of the identification instruments and using another person's identity—the provisions governing transactions concluded without authority of representation may apply by analogy. Under Section 129(1) of the *Act on the General Part of the Civil Code (Estonia)* 2002, such a transaction is void unless the person in whose name the transaction was concluded subsequently approves it (see, e.g., Supreme Court of Estonia, 2016, para. 16).

On the other hand, the Supreme Court has also adopted the view that, in such a situation, the transfer of digital-signature creation devices may, by analogy, be regarded as granting authority, with the result that a breach of instructions in the internal relationship between the transferor and the recipient has the same legal significance as a breach of the internal relationship between principal and representative (see the *Act on the General Part of the Civil Code (Estonia) 2002*, Section 131; Supreme Court of Estonia, 2019, para. 23). In the authors' opinion, however, the application of Section 131 of the *Act on the General Part of the Civil Code (Estonia) 2002* requires more than merely a breach of obligations arising from the internal relationship. The additional preconditions set out in Section 131(1) must also be satisfied: the transaction must be contrary to the interests of the represented person, and the other party to the transaction must have known or ought to have known of the breach of obligations. Furthermore, under Section 131(2), the right to avoid the transaction is excluded if the represented person knew, or ought to have known, of the circumstances giving rise to the right of avoidance and nevertheless consented to the representative's conclusion of such a transaction. The voluntary transfer of digital-signature creation devices to another person supports opinion that the owner of the identification instruments at least ought to be aware of their potential uses, thereby calling into question the right to avoid the transaction.

In addition, the Supreme Court of Estonia has found that even where the transfer of an ID card and PIN codes to another person cannot, in light of

the specific circumstances of the dispute, be regarded as granting authority, authority may nevertheless arise by operation of law, that is, on the basis of apparent authority. The situation of apparent authority is governed by Section 118(2), of the *Act on the General Part of the Civil Code (Estonia) 2002*, which provides that where the statements or conduct of a person acting as a representative reasonably lead another person to believe that authority has been granted to conclude the transaction, and the represented person knows, or ought to know, that the person is acting on his or her behalf as a representative and tolerates such conduct, the represented person is deemed to have granted authority. A person who transfers all digital-signature creation devices to another person must accept the possibility that the recipient may begin issuing signatures and declarations of intent in that person's name, and persons who conclude transactions by means of a digital signature are entitled to presume that the signatures are given by the person to whom the ID card and PIN codes were issued (Supreme Court of Estonia, 2019, para. 24).

The use of another person's ID card at a virtual meeting raises the issue of acting in the name of another; however, the legal qualification of such a situation differs from that of an ordinary contract conclusion. In the context of contract formation, a distinction must be made as to whether the identity of the counterparty was material to the other party. If it was material—for example, because the contractual obligation remains to be performed—the provisions governing the validity of contracts concluded without authority of representation apply by analogy. If, however, the identity of the other party is not material—for example, where the contract is performed simultaneously with its conclusion—the contractual party is deemed to be the person who actually made the declaration of intent, rather than the person whose identification instruments were used.

That constructions cannot be readily transferred to shareholders' meetings because the situation does not involve the creation of a bilateral contractual relationship but rather an organ procedure in which the right to participate derives from law and is strictly linked to the status of the specific shareholder. Accordingly, a user of another person's ID cannot step into the position of the shareholder or acquire an independent right to participate.

The only legally relevant question is therefore whether the use of another person's identification instrument may, in certain circumstances, justify the conclusion that a relationship of representation exists. If a shareholder knowingly transfers ID card and PIN codes to a third party, this may indicate

an intention to permit the conclusion of transactions or participation in a meeting. However, representation at a shareholders' meeting is not free in terms of its form—it must be granted at least in a form reproducible in writing (*Commercial Code (Estonia) 1995*, Section 170(3)). Consequently, the mere transfer of identification instruments may fail to satisfy the statutory formal requirement, even if it could substantively suggest an intention to grant authority. If the authorisation has not been granted in the required form, the consequence is that the representative acts without authority. In the authors' view, the formal requirement applicable to a power of attorney for participation in a meeting also precludes reliance on apparent authority (authority based on legal appearance).

The case law of the Supreme Court concerning the use of digital signatures and ID cards is primarily transferable to the allocation of the burden of proof and the presumption regarding the origin of a declaration of intent: the use of digital identification instruments creates a presumption that the act is based on the declaration of intent of the person to whom those instruments belong, and the voluntary transfer of PIN codes may preclude the argument that the identification instrument was used against the will of its owner. However, this does not alter the substantive legal requirements for representation or the applicable formal requirements. Accordingly, in the event of the use of another person's ID at a digital meeting, the actual user cannot acquire the status of a shareholder; the only question is whether representation was validly granted or whether the person acted without authority, which may entail consequences affecting the validity of the resolution adopted.

If a person uses another individual's ID card and PIN codes and, on that basis, executes a digitally signed power of attorney, which is then submitted in order to participate in the meeting, the legal structure of the situation becomes significantly more complex compared to the mere use of an ID. As noted above, the central issue is whether the authority of representation was granted in the required form. If the user of another person's identification instruments remedies that deficiency by issuing, by means of those instruments, a digitally signed power of attorney ostensibly from the actual shareholder, the focus of the dispute shifts from a question of form to a question of the existence of intent. If the power of attorney has been signed using another person's ID without the true will of the principal, this is not a case of defective form but of a forged declaration of intent. Although a digital signature creates a strong presumption that the declaration of intent originates from the holder of the certificate, that presumption is rebuttable. If it is proven that the ID card was used without the owner's consent, the

principal's genuine intent to confer authority is lacking, and no authority of representation can be deemed to have arisen. In such a case, the issue is no longer a defect in the form of the power of attorney but rather the fact that the represented person has not made the declaration of intent at all—the situation amounts to document forgery.

If, however, the owner of the ID card voluntarily transferred identification instruments and accepted their use, the situation may legally approximate tacit or implied authority, in which case it may be difficult to argue that the declaration of intent was absent. In summary, the existence of a digitally signed power of attorney may render the situation formally correct, but it does not eliminate the need to establish the principal's actual intent. If such intent is lacking, the situation constitutes acting without authority of representation, irrespective of the apparent compliance with formal requirements.

Errors in the identification of shareholders may furthermore affect the validity of resolutions adopted by the meeting. As only participants in the meeting are entitled to vote, a vote cast by a person not entitled to participate is void (unless it is subsequently ratified by the person properly entitled). This raises the question as to which legal remedy is available to a shareholder in such circumstances.

Estonian law differentiates between two types of consequences of defective resolutions: nullity (*Commercial Code (Estonia) 1995*, Section 177¹(1)) and revocation of a resolution (*Commercial Code (Estonia) 1995*, Section 178(1)). With regard to procedural defects, the guiding principle is that violations affecting shareholders' right to participate in the meeting lead to the nullity of the resolution. By contrast, infringements of other statutory provisions or of the articles of association generally constitute grounds for seeking the annulment (revocation) of the resolution rather than its nullity (Saare *et al.*, 2015, pp. 204–212). The structure of remedies against defective resolutions is, in essence, comparable under German company law. The *Stock Corporation Act (Germany)* expressly regulates the grounds for nullity (§ 241) and for revocation (§ 243). Since the *Act on Limited Liability Companies (Germany)* contains no corresponding provisions, the rules of the *Stock Corporation Act (Germany)* are applied to the *Act on Limited Liability Companies* by way of analogy (Drygala, Staake and Szalai, 2012, p. 249). Under both Estonian and German law, where a shareholder is prevented, for reasons attributable to the company, from participating in the meeting and exercising voting rights, the resolution may be deemed void (Heckschen and Kreß, 2026, p. 45; Higher Regional Court of Schleswig, 2024).

Accordingly, the question arises whether, in a situation where a person other than the shareholder participates in the meeting by using another's identification credentials, the resolution is null or merely subject to revocation. The answer follows from Section 33(3) of the *Act on the General Part of the Civil Code (Estonia) 2002*, which provides that where a vote is void, the invalidation of a resolution of a legal person's body may be sought only if the void or annulled votes affected either the possibility of adopting the resolution or its content. In the scenario described, the infringement does not amount to a violation of the shareholder's right to participate that would be classified as a defect in the convening of the meeting. Only violations of a shareholder's participation rights that are attributable to the company do give rise to nullity (Henssler and Strohn, 2024, *Act on Limited Liability Companies (Germany)* § 48 Rn. 12; BGH, 2009). A shareholder may therefore seek only the revocation of the resolution, and even then, only where the required quorum was not present at the meeting (*Commercial Code (Estonia) 1995*, Section 170(2)) or where the voting results were incorrectly determined due to the void vote (*Commercial Code (Estonia) 1995*, Section 174(1)).

6. Conclusions

The digitalisation of shareholders' meetings has not altered the fundamental premise of company law: the formation of the company's collective will is legitimate only where participation is limited to those persons who are entitled by law or by valid representation to exercise membership rights. Identity verification is therefore not a merely technical step in organising a meeting but a structural precondition for the legitimacy of the decision-making process. This normative foundation derives from the nature of participation rights themselves and is reflected, under Estonian law, in procedural requirements such as the preparation of the attendance list and the verification of quorum.

Although Estonian law contains no detailed statutory rules governing identification in virtual meetings, the admissibility of electronic participation does not modify the underlying requirement that only duly entitled persons may take part in the meeting. The transition from physical to digital meetings therefore does not change the legal standard itself but instead alters the means through which compliance must be ensured. Identity verification should be understood functionally: the measures adopted must

reliably link participation in the meeting to shareholder status or to a valid authority of representation. The virtual format renders the identification process more visible and technologically mediated, but its doctrinal objective remains identical to that in a physical setting.

The assessment of different authentication scenarios demonstrates that legal certainty varies depending on the technical and legal robustness of the identification method used. The Estonian state e-identity offers the highest degree of reliability, as cryptographically secure authentication and qualified electronic signatures create a strong and verifiable link between the individual and the declaration of intent. Where other digital identification means are employed, their reliability must be assessed individually, and weaker forms of authentication may require supplementary procedural safeguards. In the absence of any digital identification means, multilayered solutions combining prior registration, documentary verification, and real-time visual confirmation may suffice, but they inevitably entail a lower degree of certainty and a greater risk of dispute. Throughout this analysis, technological neutrality and corporate autonomy remain guiding principles, provided that the chosen solutions do not undermine the equal treatment of shareholders or the integrity of the decision-making process.

Defective identification primarily affects the validity of individual votes. A vote cast by a person not entitled to participate is void as a legal transaction. However, the consequences for the validity of the resolution as a whole depend on whether the defective vote influenced quorum or the voting result. Estonian law distinguishes between nullity and revocation: only violations attributable to the company that deprive a shareholder of the right to participate lead to nullity, whereas participation by an unauthorised person generally gives rise to the possibility of seeking revocation. The allocation of risks and burdens of proof follows the general logic of private law. The use of digital identification instruments gives rise to a rebuttable presumption that the declaration of intent originates from the holder of those instruments, yet representation at a shareholders' meeting remains subject to statutory formal requirements. The mere transfer of identification devices does not automatically satisfy the requirement of a power of attorney be granted in a form reproducible in writing, nor does it necessarily justify reliance on apparent authority.

Comparative considerations confirm that identity verification serves a procedural legitimising function and does not replace the substantive determination of membership status. The meeting itself is not the forum for

determining substantive membership status but rather a procedural setting in which the company must establish, on a sufficiently reliable basis, who is entitled to participate at the time of decision-making. Identity verification in virtual shareholders' meetings must therefore be understood as a functional mechanism of procedural legitimisation, replacing the layered safeguards inherent in physical meetings. The digital transformation of corporate governance does not require a departure from established company-law principles. Instead, it calls for their careful adaptation to a technologically mediated environment that ensures legal certainty and the integrity of collective will-formation while respecting corporate autonomy and technological neutrality. What ultimately matters is not the specific technology employed, but whether the chosen solution functionally safeguards the integrity of collective will-formation.

Andres Vutt, Dr. iur., is an associate professor of commercial law at the Faculty of Law, University of Tartu, Estonia. His work focuses on company law and corporate governance, combining academic research with teaching.

Margit Vutt, PhD in law, is a lecturer in civil law at the Faculty of Law, University of Tartu, Estonia, and a justice at the Supreme Court of Estonia. Her work centres on civil and company law, with a particular interest in private law relationships.

Maris Vutt, PhD in law, is a visiting lecturer at the Faculty of Law, University of Tartu, Estonia, and a legal counsel at Nove Law Firm. Her teaching and research relate to civil and company law.

References

Act on the General Part of the Civil Code (Estonia) 2002. Tsiviilseadustiku üldosa seadus (TsÜS). RT I 2002, 35, 216.

Altmeppen, H. (2023) *Gesetz betreffend die Gesellschaften mit beschränkter Haftung. Kommentar*. 11th edn. C.H. Beck.

Apel, S. and Nägele, T. (2025) *Beck'sche Online-Formulare. IT- und Datenrecht*. 25th edn. C.H. Beck.

BGH (2009) Bundesgerichtshof II ZR 167/07. Urteil vom 27 April, *Neue Zeitschrift für Gesellschaftsrecht*, p. 707.

Commercial Code (Estonia) 1995. *Äriseadustik* (ÄS). RT I 1995, 26, 355.

'Council directive 2007/36/EC of 11 July 2007 on the exercise of certain rights of shareholders in listed companies' (2007) *Official Journal* L 184, 14 July, pp. 17–24.

'Council regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC' (2014) *Official Journal* L 257, 28 August. Available at: http://data.europa.eu/eli/reg/2014/910/oj (Accessed: 5 August 2026).

'Council regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) *Official Journal* L 119, 4 May. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 5 August 2026).

'Council regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L 2024/1689. Available at: http://data.europa.eu/eli/reg/2024/1689/oj (Accessed: 5 August 2026).

Drygala, T., Staake, M. and Szalai, S. (2012) *Kapitalgesellschaftsrecht. Mit Grundzügen des Konzern- und Umwandlungsrechts*. Springer. Available at: https://doi.org/10.1007/978-3-642-17175-8

Fleischer, H. and Goette, W. (2026) *Münchener Kommentar zum GmbHG*. 5th edn. C.H. Beck.

Goette, W., Habersack, M. and Kalss, S. (2023) *Münchener Kommentar zum Aktiengesetz*. 6th edn. München: C.H. Beck.

Heckschen, H. and Kreß, B. (2026) 'Aktuelle Entwicklungstendenzen des Gesellschaftsrechts 2024/2025 (Teil 3)', in *Gesellschafts- und Wirtschaftsrecht*, pp. 45–51.

Henssler, M. and Strohn, L. (2024) *Gesellschaftsrecht*. Beck'sche Kurz-Kommentare. 6th edn. C.H. Beck.

Higher Regional Court of Schleswig (2024) 9 U 41/23. Judgement of 7 February 2024.

ICLEG (2022) *Report on virtual shareholder meetings and efficient shareholder communication*. August 2022. Available at: https://commission.europa.eu/system/files/2022-10/report_on_virtual_shareholder_meetings_and_efficient_shareholder_communication.pdf (Accessed: 5 August 2026).

Jerzmanowski, J. (2020) 'The growing popularity of remotely held meetings of management boards, supervisory boards and general meetings (shareholder meetings) as a manifestation of a digital revolution in company law: the case of amendments to Polish law in response to the COVID-19 pandemic', *Economics Business and Organization Research*, pp. 337–350. Available at: https://izlik.org/JA84YW59XG (Accessed: 5 August 2026).

Lange, F.-H. (2015) 'Der Leiter der GmbH-Gesellschafterversammlung', *Neue Juristische Wochenschrift*, 2015, pp. 3190–3194.

Limited Liability Companies Act (Germany) 1892. Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG). RGBl., p. 477.

Michalski, L., Heidinger, A., Leible, S. and Schmidt, J. (2023) *Kommentar zum Gesetz betreffend die Gesellschaften mit beschränkter Haftung*. 4th edn. C.H. Beck.

Noack, U., Servatius, W. and Haas, J. (2025) *Gesetz betreffend die Gesellschaften mit beschränkter Haftung*. 24th edn. C.H. Beck.

Romashchenko, I. (2026) 'Verifying shareholders for electronic participation in general meetings: law and case studies in Baltic listed companies', *Review of Central and East European Law*, 50(3–4), pp. 292–327. Available at: https://doi.org/10.1163/15730352-bja10121

Romashchenko, I. and Bitė, V. (2024) 'The electronic participation in corporate bodies in Lithuania from a comparative perspective', *Utrecht Journal of International and European Law*, 39(1), pp. 1–16. Available at: https://doi.org/10.5334/ujiel.615

Ruiu, P., Saiu, S. and Grosso, E. (2024) 'Digital identity in the EU: promoting eIDAS solutions based on biometrics', *Future Internet*, 16(7), article 228. Available at: https://doi.org/10.3390/fi16070228

Saare, K., Volens, U., Vutt, A. and Vutt, M. (2015) *Ühinguõigus* [Company law]. Juura.

Stock Corporation Act (Germany) 1965. Aktiengesetz (AktG). BGBl. I, p.1089.

Supreme Court of Estonia (2016) Case No. 3-2-1-135-16. Judgement of 21 December 2016. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-2-1-135-16 (Accessed: 5 August 2026).

Supreme Court of Estonia (2019) Case No. 2-16-124450. Judgement of 16 December 2019. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=2-16-124450/77 (Accessed: 5 August 2026).

Supreme Court of Estonia (2024) Case No. 2-23-11584. Ruling of 12 June 2024. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=2-23-11584/18 (Accessed: 5 August 2026).

Varul, P., Kull, I., Kõve, V., Käerdi, M., Saare, K. and Sein, K. (2023) *Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne* [*Act on the General Part of the Civil Code*. Annotated edition]. Juura.

Vutt, A. and Vutt, M. (2021) 'Adoption of shareholder resolutions in post-COVID era: example of Estonian law', in *New Legal Reality: Challenges and Perspectives. II: 8th International Scientific Conference of the Faculty of Law of the University of Latvia, 21–22 October 2021*. University of Latvia Press, pp. 445–458. Available at: https://doi.org/10.22364/iscflul.8.2.31

Vutt, M. (2020) 'Digital opportunities for—and legal impediments to—participation

in a general meeting of shareholders', *Juridica International*, 29, pp. 34–46. Available at: https://doi.org/10.12697/JI.2020.29.04

Vutt, M. (2024) *Legal opportunities for using digital solutions in decision-making for a limited liability company*. Doctoral thesis. University of Tartu.

Walch, A. and Häuslmeier, S. (2023) 'Die "neue" virtuelle Hauptversammlung', *Deutsche Notar-Zeitschrift*, 2023(122), pp. 106–128.

Wicke, H. (2024) *Gesetz betreffend die Gesellschaften mit beschränkter Haftung*. Beck'scher Kompakt-Kommentar. 5th edn. C.H. Beck.

Zetzsche, D.A., Anker-Sørensen, L., Consiglio, R. and Yeboah-Smith, M. (2021) 'Enhancing virtual governance: comparative lessons from COVID-19 company laws', *Journal of Corporate Law Studies*, 22(1), pp. 115–150. Available at: https://doi.org/10.1080/14735970.2021.1977453