

DIGITAL RIGHTS & CIVIL SOCIETY / EN

Digital dignity is not a privilege: Poland's Just Do It backs the OISTE Declaration

Privacy, the right to disappear and control of digital identity: why Poland's Just Do It Association backed OISTE's initiative and what it means for civil society.

TRUTH Magazine Editorial Team | 27.10.2026



TRUTH Magazine is published by the Support Center Association "Just Do It". This article develops the Association's announcement of 20 October 2025, published by Łukasz Wawrysz. The illustrations are conceptual.

At a glance

Organisation	Support Center Association "Just Do It"
Country	Poland
Initiative	Declaration of Digital Human Rights — OISTE.ORG
Decision date	20 October 2025

Digital dignity begins with a simple question: who decides what happens to the information that describes our lives? Every registration, message, search and shared document leaves a trace. Together, those traces can reveal far more about a person than they deliberately chose to disclose. Privacy is therefore a question of freedom, safety and meaningful influence over our own future, as well as a matter of information security.

On 20 October 2025, the Support Center Association “Just Do It” announced that its Board had adopted a resolution supporting the Declaration of Digital Human Rights being developed by the OISTE.ORG Foundation. The Polish NGO placed digital autonomy within its public commitments. The decision established a direction for educational work and authorised the opening of formal discussions with the Foundation about cooperation. [2]



OISTE FOUNDATION

OISTE Foundation — initiator of the Declaration of Digital Human Rights.

A Polish NGO speaks up for digital freedom

The importance of this decision extends beyond formal support for a document. Civil society organisations encounter the consequences of exclusion where technology becomes an everyday route to public services, employment and assistance. A difficult form, an incomprehensible consent request or uncertainty about a submitted document can undermine independence just as effectively as a language barrier or an inaccessible service. Digital participation depends on whether people can understand and influence the conditions under which they participate.

The Association’s position speaks to people who rely on technology without necessarily knowing how its underlying systems work. Led by Ivan-Oleksandr Yakymiv, the organisation connects a human-rights perspective with the practical realities of online life. Its resolution covers promoting the Declaration’s ideas and authorising formal discussions with OISTE.ORG. That provides a starting point for developing cooperation and practical initiatives, while keeping the focus on the needs of the people those initiatives should serve. [2]



Privacy as a boundary for informed information sharing.

OISTE: human rights must work online

OISTE's initiative draws on Article 12 of the Universal Declaration of Human Rights, which protects against arbitrary interference with privacy, family, home and correspondence. The Foundation applies that perspective to an environment in which communication, relationships and economic activity increasingly depend on data flows. Two central proposals are the right to disappear and the right to own and control one's digital identity. Together, they put personal agency at the heart of the discussion. [1]

The Declaration is the Foundation's advocacy programme and a call to improve standards for technology design and user protection. It establishes a clear ambition: privacy and autonomy should be built into the way services operate from the outset. This shifts the conversation beyond the settings of any single application. It asks developers, operators, institutions and users to consider how the broader digital ecosystem distributes responsibility and whether its arrangements give individuals an understandable and effective role.

Privacy creates room for an independent life

Privacy is sometimes reduced to keeping information secret. Its value is much wider: it allows people to choose which parts of their lives to share, with whom and in what circumstances. A doctor, an employer and a training provider need different information. Being able to keep those relationships distinct supports freedom of action and reduces the risk of being judged through material removed from its original context. Boundaries help people participate without exposing everything about themselves.

Problems arise when information supplied for one purpose circulates through additional systems and the individual loses sight of its recipients. Even seemingly minor details can become significant when combined with other records. Activity histories may reveal interests, daily routines or difficult personal circumstances. A responsible approach therefore asks why information is collected, how much is necessary and how long it should remain available. Those questions belong at the beginning of a service relationship, before inappropriate use becomes a problem.



Digital identity and personal agency.

Digital identity should preserve personal agency

Digital identity includes the information and mechanisms through which people are recognised in online services. It can involve an account, proof of an entitlement, a credential or a history of interactions. In practice, it becomes a key to participation in many areas of life. When control of that key rests entirely with a provider, a person may become dependent on arrangements they cannot easily understand, challenge or change. Access and autonomy then become closely connected concerns.

OISTE promotes an approach in which individuals manage their identity and decide how it is shared. The idea of self-sovereign identity expresses this ambition for greater independence. Its practical value can be explored through straightforward questions: does the person know what they are revealing, can they limit the information involved, and can they effectively end access? Technology has a stronger social purpose when these choices are understandable and usable by people who have no specialist technical background.

The right to disappear and the responsibility of digital memory

The right to disappear is one of the Declaration's most distinctive proposals. It addresses the ability to stop sharing information and regain influence over data that remains online. It raises important questions about second chances, changing circumstances and the limits of digital memory. Should a long-abandoned account continue exposing personal details? Can a person establish where a submitted document went? Does leaving a service actually bring specified uses of their information to an end?

In the European Union, the GDPR already provides a right to request erasure in specified circumstances. It also sets limits, including those connected with freedom of information, legal obligations and legal claims. OISTE's proposal gives the debate a broader design ambition: systems should make digital footprints easier to manage, and organisations should explain clearly what can be removed and what information they must retain. That clarity helps people understand their options and the reasons behind a decision. [3]



Control over one's digital footprint.

Consent must be understandable and control must be usable

An acceptance button cannot resolve every question of personal autonomy. People need to know what they are agreeing to and what their choice will mean. Notices should explain the purpose and scope of data use in plain language. A fair relationship also requires a practical way to change a decision. The ability to act should be visible within a service, rather than depend on finding an obscure procedure buried inside a lengthy document or navigating an unnecessarily complicated support process.

OISTE's Declaration emphasises consent, transparency and the ability to manage access. For an organisation, that direction also concerns the design of forms, settings and contact channels. A sound standard helps users make informed decisions. It can mean collecting less information, separating different purposes or explaining clearly who will receive a particular record. Transparency then becomes part of service quality and respect for the recipient. It is experienced through ordinary interactions as well as expressed in a formal policy.

Digital education as a practical form of support

The Association's announcement set out plans to promote the Declaration through workshops, training, information campaigns and educational publications. It also identified support for solutions that help individuals manage their own data. This is a programme that can be translated into useful everyday skills: recognising excessive information requests, reviewing account settings and sharing documents thoughtfully. These are tangible ways to connect broad principles with choices people face in employment, education, community work and personal communication. [2]

Effective education begins with the participant's circumstances. A jobseeker may need help assessing which information is relevant to an application. A volunteer should understand how to handle records relating to people receiving assistance. An older learner may want a patient explanation of privacy settings. These examples illustrate the range of work available to civil society: from basic habits to understanding the consequences of online decisions. Good support should increase confidence while helping people identify when they need further assistance.



Digital education: skills for everyday life.

Digital dignity also concerns civil society organisations

NGOs are part of the digital ecosystem themselves. They create forms, conduct correspondence, maintain participant lists and use external service providers. Supporting digital rights is therefore an invitation to examine their own practices. Are they requesting only the information they need? Does the recipient understand the purpose? Is it clear who can access the data and where questions can be directed? These ordinary organisational choices determine whether a commitment to dignity is reflected in the experience of the people involved.

The relationship deserves particular attention when someone is in a vulnerable situation. A person seeking urgent help should retain agency over their information. Careful handling of records and clear communication can strengthen their sense of safety. For the social sector, this is an important part of credibility: trust depends on expressed values and on everyday information practices. The quality of assistance includes the way a person is treated throughout the process, from the first request to the handling of their records afterwards.

From security to trust

Secure infrastructure is essential, but a user's experience involves more than technical protection. A service may prevent unauthorised access while leaving a person uncertain about how their information is used. Cybersecurity, transparency and accountability therefore belong together. Combined, they provide a stronger basis for deciding whether to entrust an organisation with particular data. People should be able to understand the relationship and identify a route for resolving concerns, as well as benefit from sound protection against external threats.

This connection matters for the development of the digital economy too. Trust supports cooperation, knowledge exchange and the adoption of useful new services. It requires predictable arrangements and a way to obtain explanations when something goes wrong. A human-rights perspective helps assess innovation through its effect on people's lives. Questions about technical performance should therefore be accompanied by questions about responsibility for deployment, the accessibility of safeguards and the practical ability of individuals to make their voices heard.



Trust connects security, transparency and accountability.

A position that should lead to action

The Polish Association's support for OISTE's Declaration contributes to a wider conversation about digital responsibility. Civil society can bring experience of working with people whose needs are easily overlooked in system design. It can also explain complicated issues in practical language, connecting individual rights with decisions made on a phone or computer. That contribution is valuable because meaningful participation requires more than access to a device: it also depends on understanding, confidence and a workable degree of control.

The strongest test of such a commitment is its effect on everyday life: better education, clearer procedures and greater independence for users. The resolution of 20 October 2025 established a direction for the Association's work. At its foundation is a simple principle: people should be able to benefit from the digital world while retaining dignity, knowledge about their own information and meaningful influence over their online presence. Turning that principle into accessible practice is the task that gives this initiative its social importance.

Sources and further information

1. OIste Foundation — Declaration of Digital Human Rights / Advocacy work
<https://oiste.org/what-we-do/advocacy-work/>
2. Stowarzyszenie „Just Do It” — komunikat z 20.10.2025 / original announcement
<https://www.centrum-wsparcia.pl/post/deklaracjiprawcz%C5%82owieka>
3. European Commission — Information for individuals: GDPR rights and erasure
https://commission.europa.eu/law/law-topic/data-protection/information-individuals_en?prefLang=sk

Contact

<https://www.centrum-wsparcia.pl/> | support@centrum-wsparcia.pl

Online version: <https://truthmagazine.eu/publikacje/just-do-it-oiste-digital-rights/>