Digital Rights in Practice

Personal data protection and new EU rules for digital technologies

A practical brochure for civil society organisations, activists, local authorities and interested communities in the Western Balkans

Based on the online workshop held on 24 June 2026 in Croatian, within the CROSOL project on digital literacy and responsible use of digital technologies.

Activity/publication produced within the project “Razvijanje digitalne pismenosti za predstavnike OCD-ova i lokalnih vlasti Zapadnog Balkana”, which is implemented with the financial support of the City of Zagreb.

The views expressed in this publication are the sole responsibility of CROSOL and do not necessarily reflect the views of the City of Zagreb.

CONTEXT

1. About this brochure

This brochure translates the key messages from the CROSOL online workshop Digital Rights in Practice into a practical reference for organisations and institutions that work with people, communities and digital tools. It is intended for civil society organisations (CSOs), activists, employees of local self-government units and interested participants from Montenegro, Serbia, Bosnia and Herzegovina and Croatia.

The workshop combined two connected themes: basic data protection duties in the daily work of CSOs and local communities, and the broader EU debate on digital technology regulation, including the Digital Omnibus and the Digital Omnibus on Artificial Intelligence.

How to use it

Use the brochure as a starting point for internal discussion, staff and volunteer onboarding, project planning, communication with beneficiaries, and policy monitoring. It is not legal advice and cannot replace consultation with a qualified lawyer or the competent data protection authority in your country.

Why it matters: organisations that collect data from users, members, volunteers, employees, event participants or online audiences are responsible for treating that data lawfully, fairly, transparently and securely. Digital regulation also affects the tools used for public services, advocacy, campaigning, participation, journalism and community work.

Produced with the financial support of the City of Zagreb

GDPR BASICS

2. Data protection in one page

Data protection is not only a compliance obligation. It is part of an organisational culture that respects dignity, autonomy and trust. The workshop underlined three reasons behind the adoption of the GDPR: returning control to citizens, creating consistent protection across the EU, and embedding privacy into organisational practice through the idea of privacy by design.

For countries in the Western Balkans, EU data protection standards also matter because national data protection laws are being shaped through alignment with the EU legal framework. This is relevant for cross-border cooperation, partnerships with EU organisations, public authorities and funders, and possible future adequacy discussions.

Core concepts

- Personal data: any information relating to an identified or identifiable person.
- Processing: any operation performed on personal data, including collection, storage, use, sharing or deletion.
- Pseudonymisation: data can no longer be attributed to a person without additional information.
- Anonymisation: data is processed so that re-identification is not possible.

Practical rule

- Assume information is personal data if a person can be identified directly or indirectly.
- Pseudonymised data usually still needs protection because re-identification may be possible.
- True anonymisation is difficult; be cautious when publishing datasets, photos or case descriptions.

A useful habit

Before collecting any data, ask: Why do we need it? What will we do with it? Who will access it? How long will we keep it? How will we protect it? How will we explain this to the person?

Produced with the financial support of the City of Zagreb

DAILY PRACTICE

3. Typical data processing in CSOs and local authorities

Civil society organisations and local self-government units process personal data in many ordinary activities. The fact that the work is public-interest oriented, non-profit or small in scale does not remove the need to comply with data protection principles.

CSO services and activities

- contact forms and e-mail inquiries
- free legal aid or counselling requests
- event and training registrations
- newsletter subscriptions
- campaigning, advocacy and media activities
- cookies and analytics on websites
- casework with vulnerable beneficiaries

Employees, members and volunteers

- recruitment and job applications
- payroll and legally required employment records
- members, assemblies and governing bodies
- volunteer records and contracts
- publication of staff photos or biographies
- video surveillance of offices or public premises

Local authorities may additionally process data in public consultations, youth programmes, grants, social services, local registries, public events, e-services, complaints, petitions and participatory budgeting. These activities often involve a public task or legal obligation, but transparency, minimisation and security still apply.

Do not collect “just in case” data

A registration form for a workshop usually does not need a personal identification number, date of birth, full address or sensitive information. Collect only what is necessary for the stated purpose.

Produced with the financial support of the City of Zagreb

4. Choosing a lawful basis

Every processing activity needs a lawful basis. No lawful basis is automatically “better” than the others: the right basis depends on the purpose, the organisation’s role, the relationship with the person, and the applicable national law. The choice should be made before processing starts and documented internally.

Six lawful bases

- consent
- contractual necessity
- legal obligation
- vital interests
- public interest / public task
- legitimate interest

Examples discussed in the workshop

- Legal obligation: employee, member and volunteer records required by law.
- Contract: membership application or free legal aid/service relationship.
- Legitimate interest: some forms of video surveillance, staff photographs or journalistic activity, subject to balancing and safeguards.
- Consent: newsletter subscriptions and non-essential cookies.

Consent is not a shortcut

Consent must be freely given, specific, informed and unambiguous. It should be as easy to withdraw as to give. Avoid consent where there is a strong imbalance of power or where another legal basis is more appropriate.

Important: examples above are illustrative. National rules may be stricter, especially for employment, public authorities, video surveillance, children, health data, or social services.

Produced with the financial support of the City of Zagreb

5. Six principles for everyday compliance

Lawfulness, fairness and transparency
Have a legal basis, process data in a way people would reasonably expect, and provide clear information about the processing.

Purpose limitation
Collect data for specific, explicit and legitimate purposes. Do not later reuse it in an incompatible way.

Data minimisation
Process only data that is adequate, relevant and necessary for the purpose.

Accuracy
Take reasonable steps to keep data accurate and correct or delete inaccurate data without delay.

Storage limitation
Keep identifiable data only for as long as necessary for the purpose or as required by law.

Integrity and confidentiality
Protect data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Produced with the financial support of the City of Zagreb

SENSITIVE INFORMATION

6. Special category data requires extra care

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic and biometric data, and data concerning sex life or sexual orientation. These categories are especially relevant for many CSOs because human rights, social inclusion, health, minority rights, gender equality and democracy work often involves sensitive contexts.

Under GDPR Article 9, processing special category data is in principle prohibited unless a specific exception applies. One exception may apply to foundations, associations or other non-profit bodies with political, philosophical, religious or trade union aims when processing is part of their legitimate activities, relates to members, former members or persons in regular contact, adequate safeguards are in place, and data is not disclosed outside the organisation without consent.

Good practice

- collect sensitive data only when truly necessary
- separate sensitive records from general contact lists
- limit access to trained staff only
- use encrypted storage for files and devices
- avoid publishing identifying details in case studies
- document which Article 9 or national-law exception applies

High-risk examples

- lists of beneficiaries by health status or ethnicity
- political affiliation inferred from event attendance
- records of survivors of violence or discrimination
- photos or stories revealing a person's migration, health or minority status
- AI tools used to profile vulnerable groups

Produced with the financial support of the City of Zagreb

WHO IS RESPONSIBLE?

7. Roles and accountability

Data protection work becomes easier when roles are clear. Organisations should know when they decide the purposes and means of processing, when they process data on behalf of someone else, and when another organisation is acting as a processor for them.

Main roles

- Controller: decides why and how personal data is processed.
- Processor: processes personal data on behalf of the controller.
- Supervisory authority: independent public body responsible for monitoring and enforcing data protection law.
- Data Protection Officer: advises and monitors compliance where a DPO is required or appointed.

Typical arrangements

- an NGO as controller for event registrations
- an online newsletter platform as processor
- a municipality as controller for a public consultation
- a cloud service or IT support company as processor
- joint work with partners requiring clear allocation of roles

What a Data Protection Officer does

A DPO advises the organisation about legal obligations, monitors compliance with law and internal policies, cooperates with the supervisory authority, supports individuals in exercising their rights, advises on data protection impact assessments, and acts independently and without conflict of interest.

Even when a DPO is not legally required, it is useful to name a responsible person or team for data protection questions, breaches and internal procedures.

Produced with the financial support of the City of Zagreb

8. Individual rights and data breaches

People whose data you process have rights. In practice, your organisation should know how to receive, record, verify and respond to requests from individuals.

Rights of individuals

- right of access to personal data
- right to rectification of inaccurate data
- right to data portability
- right to erasure
- right to restriction of processing
- right to object to processing
- right not to be subject to fully automated decision-making in certain cases

Data breach response

- A breach is a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Inform the responsible person immediately.
- Assess risk to individuals and document the incident.
- Notify the supervisory authority within 72 hours when required.
- Inform affected individuals without undue delay when the risk is high.

Prepare before something happens

Have a short breach-response procedure: who receives incident reports, who decides whether to notify the authority, who communicates with affected people, and where the breach log is kept.

Produced with the financial support of the City of Zagreb

FOR CSOS AND LOCAL AUTHORITIES

9. Practical data protection checklist

Map your main processing activities: participants, members, volunteers, staff, beneficiaries, website users, partners and suppliers.

Define the purpose and lawful basis for each activity.

Remove unnecessary fields from forms and databases.

Prepare clear privacy notices for events, newsletters, consultations, services and websites.

Keep consent separate from other terms and keep proof of consent when consent is used.

Adopt a retention schedule and delete or anonymise data when it is no longer needed.

Sign processor agreements with IT, cloud, mailing, survey or event-management providers.

Limit access to sensitive records and review permissions regularly.

Use strong passwords, multi-factor authentication and secure storage for files and devices.

Keep a breach log and test your breach-response procedure.

Train employees, volunteers and project partners who handle personal data.

Review public communications, photos and case studies before publication.

Use AI tools only with clear rules: no confidential, beneficiary or sensitive personal data in public or uncontrolled tools.

Produced with the financial support of the City of Zagreb

DIGITAL POLICY

10. EU digital regulation: the bigger picture

EU digital regulation is not a single law. It is a growing framework of rules on data protection, law enforcement data, platforms, markets, data access, cybersecurity and artificial intelligence. The workshop placed the Digital Omnibus debate in this wider regulatory landscape.

Instrument	Main focus	Why it matters for CSOs/local authorities
GDPR	Personal data protection	Privacy notices, legal bases, rights, security, breaches, accountability.
LED	Data protection in law enforcement	Relevant where police, public security or justice-sector data is involved.
DSA	Online platforms and content governance	Platform transparency, systemic risks, content moderation and online civic space.
DMA	Digital market gatekeepers	Competition, access and power of very large platforms.
Data Act / data rules	Access to and use of data	Data sharing, interoperability and data-driven services.
AI Act	Risk-based rules for AI systems	AI literacy, transparency, high-risk systems and public-sector uses of AI.
NIS2 / cybersecurity	Cybersecurity obligations	Security culture, incident reporting and resilience of services.

For smaller organisations and local authorities, the challenge is often not one regulation, but the cumulative effect of several overlapping frameworks, platforms, procurement choices, cloud services, AI tools and public expectations.

Produced with the financial support of the City of Zagreb

SIMPLIFICATION OR DEREGULATION?

11. Digital Omnibus and AI Omnibus

In November 2025, the European Commission presented a Digital Package aimed at simplifying parts of the EU digital rulebook. The package includes proposals known as the Digital Omnibus or Data Omnibus, and the Digital Omnibus on Artificial Intelligence. Commission materials describe the objective as simplification, reducing overlapping obligations and supporting innovation and competitiveness.

The AI Omnibus entered into force across the EU on 27 July 2026. It introduces targeted simplification measures and extended timelines for some AI Act obligations. The wider Digital Omnibus debate also concerns data, cybersecurity and elements of AI regulation.

Commission framing

- simplify and consolidate the digital rulebook
- reduce administrative burdens and overlaps
- support innovation and competitiveness
- align data, cybersecurity and AI obligations
- make reporting easier through common or single-entry procedures

Civil society concerns highlighted in the workshop

- possible narrowing of rights and safeguards
- expansion of exceptions or non-application of rules
- reduced transparency obligations
- delays in legal obligations
- limited participation of ombuds institutions, CSOs and trade unions
- strong influence of large technology companies

Balanced reading

The same proposal can be presented as administrative simplification by institutions and as deregulation or rollback by rights-based organisations. For CSOs and local authorities, the key question is whether simplification makes compliance easier without weakening protection for people.

Produced with the financial support of the City of Zagreb

RIGHTS AND PUBLIC INTEREST

12. Why civil society and local authorities should pay attention

Digital rules shape the environment in which organisations communicate, mobilise, provide services, collect evidence, participate in public debate and use technology. They also shape how local public services can adopt AI, digital identity, automated systems and data-driven tools.

Risks to watch

- weaker transparency can make it harder to understand automated or platform decisions
- broad exceptions can increase use of personal or sensitive data without meaningful safeguards
- longer implementation timelines can delay practical protections
- complex rules can disadvantage smaller organisations and municipalities
- private technology providers can gain influence over public-interest infrastructures

Opportunities for action

- build internal digital-rights knowledge
- participate in consultations and public debates
- ask for fundamental-rights impact assessments in public-sector AI projects
- cooperate regionally and exchange examples of responsible technology use
- include digital rights in advocacy, local policy and civic education work

Policy-monitoring questions

Who benefits from the proposed simplification? Which obligations are being delayed or removed? Are affected communities consulted? Is there an impact assessment? Are transparency, redress and oversight still strong enough? What does the change mean for vulnerable groups?

Produced with the financial support of the City of Zagreb

INTERNAL RULES

13. Responsible use of digital and AI tools

Digital tools and AI systems can help organisations save time, communicate better and analyse information. They can also create risks when used without rules, especially when personal data, sensitive communities or public decisions are involved.

Before using a tool

- define the purpose and expected benefit
- check whether personal or sensitive data will be processed
- read the provider's privacy and data-use terms
- decide who may use the tool and for what tasks
- avoid uploading confidential case files, beneficiary data or unpublished sensitive documents
- assess accessibility, language and bias risks

When using AI outputs

- keep human oversight and final responsibility
- fact-check outputs against reliable sources
- do not use AI as the only basis for decisions affecting people
- be transparent when AI substantially shaped public communication or analysis
- protect copyright, confidential information and personal data
- keep records for important decisions and policy work

A simple internal AI rule

No staff member, volunteer or external collaborator should enter personal data of beneficiaries, users, members, complainants, employees or volunteers into public AI tools unless the organisation has assessed the tool, documented a legal basis and implemented appropriate safeguards.

Produced with the financial support of the City of Zagreb

ADAPT INTERNALLY

14. Useful mini-templates

Privacy notice skeleton for events

- Who is the controller? Name the organisation and contact address.
- What data is collected? For example: name, e-mail, organisation, country, accessibility needs.
- Why is it collected? Registration, event communication, reporting, participation records.
- What is the lawful basis? Define it clearly.
- How long is data kept? Define a retention period.
- Who receives the data? Event platform, project team, funder only in aggregate unless otherwise justified.
- What are the participant's rights and whom can they contact?

Data breach log fields

- date and time discovered
- what happened and which systems/files were affected
- categories and approximate number of people affected
- categories of data involved
- initial containment measures
- risk assessment
- decision on authority/individual notification
- follow-up measures and lessons learned

AI use register fields

- tool name and provider
- purpose and users
- types of data entered
- risks and safeguards
- human review steps
- date reviewed and responsible person

Produced with the financial support of the City of Zagreb

REFERENCE MATERIAL

15. Sources and further reading

This brochure is based on the workshop presentations prepared for CROSOL's online workshop "Digitalna prava u praksi" held on 24 June 2026, the CROSOL project documentation, and selected official and civil society sources listed below. Online sources were checked in August 2026.

1. Workshop materials: "Zaštita osobnih podataka", CROSOL workshop presentation, 24 June 2026; "Regulacija digitalne tehnologije u EU", Politiscope workshop presentation, 24 June 2026.

2. Project documentation: CROSOL project "Razvijanje digitalne pismenosti za predstavnike OCD-ova i lokalnih vlasti Zapadnog Balkana".

3. European Commission, Data protection explained: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

4. European Commission, Application of the GDPR: https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/application-gdpr_en

5. European Commission, Legal grounds for processing data: https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/legal-grounds-processing-data_en

6. European Commission, What is a data breach and what do we have to do in case of a data breach?: https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en

7. European Data Protection Board, Personal data breaches: https://www.edpb.europa.eu/topics/security-data-breaches/personal-data-breaches_en

8. EUR-Lex, Regulation (EU) 2016/679 - General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

9. European Commission, Digital Package: https://digital-strategy.ec.europa.eu/en/faqs/digital-package

10. European Commission, Simpler digital rules to help EU businesses grow: https://commission.europa.eu/news-and-media/news/simpler-digital-rules-help-eu-businesses-grow-2025-11-19_en

11. European Commission, An agile Digital Rulebook for the EU: https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook

12. EUR-Lex, Digital Omnibus on AI adopted text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3APE_30_2026_REV_1

13. BEUC and partners, Open Joint Letter on the Digital Omnibus on AI, 8 April 2026: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-029_Open_Joint_Letter_on_the_Digital_Omnibus_on_AI.pdf

Legal note

This publication is an educational resource. It provides general information and practical orientation, but it does not constitute legal advice. Always check the legislation and guidance applicable in your jurisdiction.

Produced with the financial support of the City of Zagreb

VISIBILITY

16. About the project

This brochure was created as part of CROSOL's project focused on strengthening digital literacy and responsible use of digital technologies among civil society organisations and local authorities in the Western Balkans. The activity builds on CROSOL's cooperation with organisations and networks in the region and on expertise provided by Politiscope in the fields of digital rights, EU technology regulation and responsible use of contemporary technologies.

Donor visibility statement

Activity/publication produced within the project "Razvijanje digitalne pismenosti za predstavnike OCD-ova i lokalnih vlasti Zapadnog Balkana", which is implemented with the financial support of the City of Zagreb.

The views expressed in this publication are the sole responsibility of CROSOL and do not necessarily reflect the views of the City of Zagreb.

CROSOL - Croatian Platform for International Citizen Solidarity
www.crosol.hr

August 2026