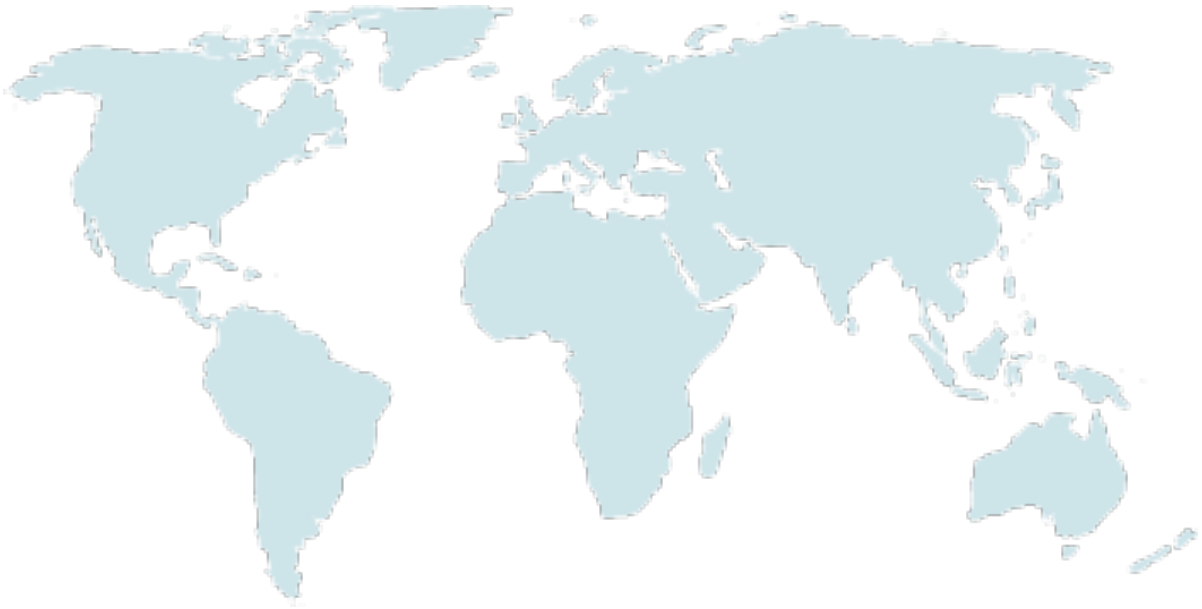
ICNL

www.icnl.org
info@icnl.org

OVERVIEW

Kyrgyzstan: Understanding and Complying with Personal Data Laws



INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

1660 L Street NW #600
Washington, DC 20036

Table of Contents

This guidance note is designed for civil society organizations (CSOs) in Kyrgyzstan that collect, store, or use personal data in their work. Common examples include registering participants for events, managing mailing lists, keeping staff files, or sharing reports with donors. These are only a few illustrations; personal data processing can take many other forms. If your organization handles personal data in any way, you must comply with the law. This note explains the rules in plain language and provides practical steps, examples, and checklists to support CSOs in meeting their obligations.

Kyrgyzstan's personal data framework is undergoing significant reforms:

- The Law on Personal Information, adopted in 2008, continues to provide the basic rules for handling personal data and will remain in force until February 8, 2026.
- In parallel, amendments to the Code on Offenses, adopted on May 19, 2025, introduced fines for a wide range of violations of personal data protection requirements. These provisions will take effect on November 23, 2025.
- On July 31, 2025, the President signed the new Digital Code, which modernizes data protection rules and removes the obligation for organizations to register as personal data holders. Once it enters into force on February 8, 2026, the Digital Code will replace the Law on Personal Information in its entirety.

This creates a short but important transition period between November 23, 2025, and February 8, 2026, when the requirements of the Law on Personal Information will continue to apply and organizations may still face fines for violations, including processing personal data without proper registration. CSOs must therefore ensure full compliance with the current law while preparing for the new framework that will apply from February 2026 onward. To support organizations during this period, ICNL developed this guidance note, and will later produce an updated resource to help CSOs adapt to the Digital Code once its provisions on personal data protection come into effect.

Complying with data protection rules is not only about avoiding penalties, but also respecting individual privacy, protecting beneficiaries from harm, and building trust between communities, donors, and partners. Responsible handling of personal data demonstrates professionalism, strengthens your organization's reputation, and helps ensure that projects do not cause unintended harm.

Data Protection Requirements at a Glance

√ **Identify the personal data you handle.** This includes names, contacts, ID/passport numbers, photos, videos, emails, and similar information. Sensitive data (such as religion, ethnicity, health, sexual orientation, or political views) requires extra care. Collecting or using sensitive data is generally prohibited, unless there is a strong justification.

√ **Have a lawful basis for processing.** In most CSO activities, this will be consent. Be clear and transparent about why you collect the data and how it will be used.

√ **Collect and document consent properly.** Consent can be written or electronic. Separate consent is needed for each purpose (e.g., newsletters, photos, donor sharing). People may withdraw their consent at any time. Consent must clearly state:

- Who is collecting the data (your CSO)
- What data is being collected
- Why it is being collected
- How it will be used
- With whom it will be shared (specific third parties)
- How long it will be kept

√ **Apply core data protection principles:**

- Collect only what you need.
- Keep data accurate and secure (passwords, access controls, locked cabinets).
- Store data only as long as necessary, then securely destroy it.
- Do not merge or repurpose data sets without a legal basis or new consent.
- Respect confidentiality unless the data is anonymized or the person has agreed to make it public.

√ **Be careful with cross-border data transfers.** Using tools like Google Forms, cloud storage, or sending participant lists to donors abroad counts as transferring data outside Kyrgyzstan. Until the official list of countries with "adequate protection" is published, always obtain explicit consent before transferring personal data abroad.

What is Personal Data?

> Article 3 of the Law on Personal Information

Personal information (or personal data) is any information about a person that can be used to identify them directly or indirectly. This includes names, physical addresses, passport and national ID numbers, video or voice recordings, photographs, fingerprints, email addresses, internet protocol (IP) addresses (*unique number associated with devices like computers and mobile phones that connect to the internet*), genetic data, and any other data that is ascribed to a specific individual. The information can either be:

- One piece of information that can be directly linked to a person, or
- Multiple pieces of information that can be combined to discern the identity of a person.

If information can be used to recognize a specific person, it is considered personal data and is protected by law. However, if the data is "depersonalized," it is no longer considered personal data. Depersonalization means that all identifying information is removed and erased altogether. Encrypting personal data or coding and storing different pieces of data separately are not considered full depersonalization.

The individuals who are identified in the datasets are called **data subjects**. The Law grants rights to data subjects over their personal data.

EXAMPLE

Birge Civic Initiative (BCI) employs 15 staff. For each employee file, BCI collects and stores the individual's full legal name, national tax ID number, date of birth, home address, phone number, and emergency contact name and number for a family member. BCI also works with volunteers on Saturday mornings. When they arrive, the volunteers sign in and when they leave, they sign out. At the end of the day, BCI tallies the number of volunteers that arrived and the total number of hours they worked. The sign in sheet is then shredded and discarded.

Is this personal data?

Employee records: Yes. The information in personnel files clearly identifies individual staff members (names, contact details, ID numbers, etc.). This is personal data, and BCI must comply with the personal data protection law when collecting, storing, and using it.

Volunteer statistics: No. The final tally of "15 volunteers worked a total of 45 hours" does not identify anyone personally. Because the data has been depersonalized, the data protection law would not apply.

What is Sensitive Personal Data and How Should It Be Handled?

> Article 8 of the Law on Personal Information

Some types of personal data are considered especially sensitive. Collecting or using them is generally prohibited, unless there is a strong justification. These include data that reveal a person's race or ethnic origin, nationality, political views, religious or philosophical beliefs, health status, sexual orientation. Importantly, the law forbids collecting or using this data just for the purpose of identifying these traits.

CSOs can process such data only in two cases:

- With the person's explicit consent. Example: A beneficiary agrees in writing to share their medical history for participation in a health project.
- For urgent protection of health or safety, when consent cannot be obtained. Example: In an emergency situation (such as a medical crisis during an event), sharing information about a person's health with a doctor to save their life.

Collecting or publishing information about someone's political, religious, ethnic, or sexual identity without their permission is against the law. Even if a person belongs to a vulnerable group that your project supports (e.g., people with HIV, survivors of violence, ethnic minorities), you must not record or disclose this information unless they have freely given informed consent, or it is strictly necessary to protect someone's life or safety.

NOTE FOR CSOS

- √ Always ask yourself: Do we really need this sensitive information to achieve our goal? If not, do not collect it.
- √ If you do need it, make sure you have clear, written consent and strong security measures in place.
- √ Remember: protecting sensitive data is not only a legal duty but also an ethical responsibility to safeguard the trust of your beneficiaries.

EXAMPLE

BCI's policy states that any employee who belongs to a religious minority can take leave to observe religious holidays and practices. To take advantage of this benefit, the policy stipulates that the employee must send an email to request approval from BCI's Director with information about the religion, the religious holiday, and why the leave is needed to observe the holiday. This email is then saved in the employee's file.

Should BCI change its procedures for recording employee requests for days off?

Yes, BCI should change its procedures. Information about an employee's religion is considered sensitive personal data under the Law on Personal Information, and collecting or storing it creates legal risks. Requiring employees to explain their religion and religious holidays means BCI is unnecessarily collecting sensitive data.

Are there other procedures BCI could adopt to avoid collecting sensitive personal data?

BCI could update the policy so that employees only need to request "leave for personal reasons" or "leave for religious observance," without mentioning the religion or details of the holiday. The organization could record only the date(s) of leave and the type of leave (annual, unpaid, special leave, etc.) in the employee files and avoid storing any information that reveals the employee's religious beliefs. This way, employees can still enjoy their rights and benefits, while BCI avoids the risks of processing sensitive personal data.

What is Data Processing?

> Article 3 of the Law on Personal Information

Processing is a broad concept. It includes any handling of personal data whether it is done by hand or through the use of a computer. Processing covers the full life cycle of personal data — from the moment you collect it, to the time you store, update, or delete it.

EXAMPLE

Your CSO is processing personal data when you:

- collect names and contact details during event registration;
- store scanned copies of passports for travel support;
- update your mailing list with new emails or phone numbers;
- group beneficiaries by age, sex, or region for a project report;
- block access to sensitive files using passwords;
- erase outdated event registration forms; and
- destroy old paper records with personal information.

If your organization does any of the abovementioned (or other comparable activities), you are processing personal data and must follow the rules under the law.

Who is Obligated to Comply?

> Article 3 of the Law on Personal Information

Holder (owner) of a personal data set is the organization that oversees and directs the handling of personal data. The holder (owner) decides why the data is being collected

(the purpose), what kind of data is collected, and how the data will be used and protected. If your CSO collects personal data for its work (e.g., for a project, event, or service), your CSO is the holder (owner) of that data. You are responsible for making sure it is used lawfully and securely.

In turn, a *data processor* is someone who helps you handle personal data on your behalf but only under a contract and according to your instructions. This could be an IT company that manages your database, a consultant who analyzes survey responses, or a printing service that prepares personalized certificates for your beneficiaries. The processor does not decide what to do with the data. Rather, they take direction from the holder (owner).

EXAMPLE

BCI runs a youth training program and collects participants' names and emails for monitoring and reporting purposes. BCI hires an event agency to organize the program, and the agency manages the registration table outside of the training room. Following the training, BCI uses an online survey tool to collect participant feedback. The tool is free service offered by an online platform, but BCI has a platform account so it can use the service.

Is BCI a holder (owner) or processor? Why?

BCI is the holder (owner). It decided to collect personal data, it decided how the data will be used, and it required that certain types of personal data be collected.

Is the event agency a holder (owner) or processor? Why?

The event agency is a processor. It is working on behalf of BCI and taking directions from BCI on what personal data to collect and how.

Is the survey platform a holder (owner) or processor? Why?

The survey platform is a processor in this instance. Even though it offers a free service, it is still collecting and storing data on behalf of BCI. Note that the survey platform is likely a holder (owner) with regards to the name, email, and IP address of the staff member at BCI who manages the account.

What Types of Data Processing Fall Outside the Scope?

> Article 2 of the Law on Personal Information

The law covers almost all situations where personal data is handled – no matter whether it is done on paper or using digital tools, or whether it is done by a company, a public institution, or an individual.

However, there is one important exception: the law does not apply when an individual processes personal data for purely personal, family, or household purposes, as long as no one's rights are violated. Thus, the law does not regulate private, non-professional activities.

When a CSO collects or uses personal data as part of its organizational activities, such as projects, services, or events, the law applies even if the data is only handled by one staff member or in a small-scale setting. A CSO **cannot** claim the "personal use" exception.

EXAMPLE

The wife of BCI's Executive Director attends a staff party and takes a group photo. She prints a copy and hangs it in a frame at home. The Executive Director sees the photo and decides it should be posted on the homepage of BCI's website.

Does the Law on Personal Information Apply to the Photo?

When the Executive Director's wife hangs the photo in a frame at home, this falls under the personal use exception, and the Law on Personal Information should not apply. However, if the Executive Director posts the photo on the website, the Law becomes applicable. Therefore, he should not post the photo online before he secures consent from everyone depicted in the photo.

What are the Main Principles of Personal Data Protection?

> Article 4 of the Law on Personal Information

Under Article 4 of the Law on Personal Information, CSOs must follow a set of key principles when handling personal data:

1. *Legality:* Before handling personal data, CSOs must ensure there is a legal basis for personal data processing and that they are prepared to comply with the rules and procedures established in the law.
2. *Transparency and Purpose Limitation:* CSOs must be clear and transparent about the purpose of data collection. They must only collect personal data for the purpose originally communicated at the time of collection. For instance, if a CSO collects data for event registration, it cannot add the participants' contact information to a fundraising mailing list without first seeking consent for the new purpose.
3. *Accuracy:* When CSOs collect and store personal data, the data must be kept up-to-date, and individuals must be able to request rectification if the data is inaccurate. This obligation is particularly important when data subjects are likely to be negatively impacted if their personal data is inaccurate. For

example, CSOs have the responsibility to ensure that employee files are accurate and updated on a regular basis. If an employee's ID number or address is not input into the physical or digital file correctly, it could impact their payments or delivery of tax documents. The original data must be accurate and, where necessary, kept up to date.

4. *Storage Limitation:* Personal data should only be kept for as long as it is needed for the purpose it was collected. Once that purpose has been achieved, the data must be securely destroyed.[1] CSOs should avoid keeping outdated participant lists, application forms, or similar records indefinitely. If a project has ended and the personal data is no longer necessary, it should be properly disposed of securely.
   - However, certain documents must be retained for specific periods as required by law. For example, personnel records that document an individual's employment history (such as personnel orders on hiring or dismissal, employment contracts and agreements, or payroll registers) must be kept for 60 years.
   - For detailed guidance, CSOs should refer to the List of Standard Administrative Archival Documents Generated in the Course of Activities of State and Non-State Organizations, Indicating Their Retention Periods. This is the primary regulatory document for determining how long different types of records must be retained and for selecting documents for either destruction or permanent storage in state archives. In addition to this regulation, a CSO should consult any other applicable laws to determine if and how long a document containing personal data should be retained.
5. *Integrity:* If personal data is kept for historical or other long-term reasons, there must be strong protections in place. If CSOs are archiving project records for reporting or research, you must ensure proper security measures (e.g., encryption, restricted access).
6. No unlawful combination of data sets: Combining data sets for new automated uses is prohibited. You cannot merge different personal data sets (collected for different purposes) and process them together using automated systems. If a CSO collected data separately for a women's health project and for a youth

[1] "Secure destruction" means making sure personal data cannot be restored or read again once it is no longer needed. For paper records, this usually means shredding or burning. For electronic files, it means using software that permanently deletes the file (not just moving it to the recycle bin) or physically destroying the storage device if necessary. The goal is to prevent anyone from being able to recover or misuse the data later.

leadership program, you cannot combine the two databases and run automated analysis unless you have a legal basis and informed consent.

7. Confidentiality: Personal data must be stored securely and protected from unauthorized access, changes, or deletion. CSOs should use password protection, secure storage (physical or digital), and access controls. Ensure that only authorized individuals have access to and handle personal data.

These principles are not exhaustive. New principles may be added based on future legal developments in the Kyrgyzstani law. Therefore, CSOs should stay informed about updates to data protection laws and be prepared to adapt their practices.

When You Need to Get Consent to Collect or Use Personal Data

> Article 5 of the Law on Personal Information

Consent is one of the main legal grounds that allows an organization to process personal data lawfully. By securing consent, CSOs can process personal data without being obligated to show that one of the other legal bases for processing applies. Consent protects both the rights of individuals and your organization's credibility and legal compliance. The next section describes the standards and procedures for obtaining consent.

How to Obtain Consent for Collecting and Processing Personal Data

> Article 9 of the Law on Personal Information
>
> *See also* the Procedure for Obtaining the Consent of a Personal Data Subject for the Collection and Processing of Their Personal Data, including in the Form of an Electronic Document, and for the Purposes of Providing State and Municipal Services (hereinafter – Order N27)

There are rules and requirements for obtaining a person's consent before collecting or using their personal data:

1. To ensure that data subjects consent knowingly and freely, CSOs should ensure that the data subjects are clearly informed that their personal data is being collected at the time of collection.
2. CSOs must always document consent in writing – either on paper in a non-digital format or as an electronic document signed in accordance with the Law

on Electronic Signature.[2] Consent given electronically may also be recorded through actions such as entering a login and password, ticking a checkbox, or clicking an "accept" button, provided that reliable proof of this action is stored.

3. To ensure there is "informed" consent, CSOs must explain the following information in plain language:
   - Who is the entity collecting the data (e.g., a CSO's name, address, and contact details).
   - The type of data being collected (e.g., name, phone number, photo, email).
   - The purpose of collection (e.g., event registration, mailing list, service delivery, donor reporting).
   - The anticipated uses of personal data (e.g., storage, posting on social media, inspections by a third-party tax auditor).
   - The (third-party) entities that will receive the data (e.g., specific names of donors, CSOs, government offices, vendors; be sure to avoid vague phrases like "other partners").
   - The duration of the consent (e.g., a specific date, period, or other clear criteria). If the duration of consent differs for each purpose, it must be specified separately for each purpose.
4. A person can refuse to provide their data and withdraw consent at any time, and they do not need to provide a reason. There are exceptions in cases when CSOs are legally or contractually required to keep the data, but generally, CSOs should be prepared to fully erase all personal data upon a request from the individual who is the subject of the data.
5. The CSO must be able to prove that it obtained consent properly. If the consent is questioned, the responsibility to prove it lies with the CSO (the data holder). This means CSOs must keep proper records of signed consent forms or electronic confirmations.

Important: You cannot ask for "blanket consent" for all purposes and uses of data. Each separate purpose (e.g., sharing with a donor, posting photos online, cross-border transfer) requires its own specific consent.

[2] Law on Electronic Signature: https://cbd.minjust.gov.kg/111635/edition/985628/ru.

Checklist for CSOs on Fulfilling the Requirement to Obtain Consent

Ask yourself the following questions to make sure you fulfill the legal requirements of obtaining consent:

- √ Do we have a consent form when collecting personal data (in paper or electronic format)?
- √ Do we clearly explain the purpose of data collection?
- √ Does our consent form list all required details (who, what, why, how, how long)?
- √ Do we obtain separate consent for each purpose?
- √ Do we allow free choice? If there are several purposes of data collection, is the person able to agree to some purposes and refuse others?
- √ Do we securely store proof of consent for as long as the data is used?
    - Do we keep a signed paper copy?
    - Do we keep signed e-documents or maintain logs or registers?
    - Do we destroy records when they are no longer needed?
- √ Do we inform individuals of their rights and how to withdraw consent?

NOTE FOR CSOS

For event registration: Use a form with separate checkboxes so participants can choose individually whether they agree to (a) attend the event, (b) receive newsletters, (c) be photographed or recorded, etc. Example wording:

- *I will participate in the event*
- *I would like to receive newsletters and updates from [Organization Name]*
- *I agree to be photographed and/or recorded during the event*

For online forms: Collect consent through an online form where participants provide their email, read a short privacy notice, and click "I agree." Make sure to keep the timestamp as proof of consent. Example wording:

> *"By clicking "I agree," I confirm that I have read the privacy notice and consent to [Organization Name] processing my personal data for the purposes described."*
>
> *Note: For any online engagement and data gathering, keep in mind that many services collect IP addresses. If you do not need IP addresses for any purpose, either disable the feature or ensure they are deleted at the time of collection. If the IP*

addresses are recorded for a specific purpose, inform the data subjects and explain the purpose.

For photos and videos: Ask participants to sign a separate consent form specifically for the use of their images in reports, on websites, or on social media. Example wording:

I agree to the use of my photo/video by [Organization Name] in publications, reports, and on social media. I understand that my image will not be used for commercial purposes.

- *I agree*
- *I do not agree*

Sharing data with donors: If participant data will be shared with a donor, clearly name the donor in the consent form and explain the purpose of sharing. Example wording:

Your name, organization, and email will be shared with our donor, [Donor Name], to demonstrate project results and maintain transparency. Your data will not be used for other purposes.

- *I agree to my data being shared with [Donor Name]*
- *I do not agree*

RESOURCES AND TEMPLATES

Model consent form (in development): The DPA is preparing a standard consent form. Check their official website for updates: dpa.gov.kg.

Existing template: The Annex to Order N27 contains a model consent form mandatory for state and municipal bodies. CSOs can adapt this template for their own events and activities.

Cross-Border Transfer of Personal Data: What It Means and How to Stay Compliant

> Article 25 of the Law on Personal Information

Many CSOs in Kyrgyzstan work with international partners, donors, and networks. This often requires sharing personal data across borders – for example, sending participant lists to a donor abroad, using a cloud storage service or other software service that hosts data in servers in other countries, or sharing passport or other travel documents to hotels and airlines outside of Kyrgyzstan, or even physically taking documents and papers that contain personal data in luggage when attending conferences or events abroad. Article 25 sets the rules for when and how such transfers are allowed.

Under Article 25 of the Law on Personal Information, a CSO may only transfer personal data to another country if that country has strong data protection rules (an "adequate level of protection"). If the country you want to send data to does not have adequate data protection laws, the transfer is only allowed in special cases:

- With the consent of the person – e.g., if a participant agrees in writing that their data can be shared with a foreign partner.
- To protect the person's interests – e.g., sharing medical details in an emergency.
- If the data is already public – e.g., names and contacts listed in a public directory or on a public website.

NOTE FOR CSOS

A practical challenge is the current absence of official guidance on which countries meet the "adequate protection" standard. The Data Protection Agency (DPA) plans to publish a list of such countries; however, this list has not yet been issued. In the meantime, CSOs are not in a position to make an authoritative determination as to whether the legal framework of another state provides a level of protection equivalent to that of Kyrgyzstan.

Therefore, to demonstrate good faith compliance while awaiting clearer instructions from the DPA, CSOs should always include information about cross-border data transfers in their consent forms and obtain informed consent from individuals whose data may be transferred.

When is Personal Data Confidential and When Can It Be Made Public?

> Article 6, 7, and 26 of the Law on Personal Information
>
> *See also:* Order of the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic on the Approval of the Procedure for the Anonymization of Personal Data for the Purposes of Conducting Statistical, Sociological, Historical, Medical, and Other Scientific and Practical Research dated January 14, 2025, No. 4.

Personal data is considered confidential information unless the law says otherwise. This means CSOs must handle it carefully, keep it private, and protect it from misuse. If your organization collects names, addresses, phone numbers, or other personal details of beneficiaries, staff, or partners, you must treat this information as private. You must put in place safeguards to prevent unauthorized access, blocking or withholding

information unlawfully, unlawful transfer, accidental or unauthorized destruction, alteration, or loss.

Confidentiality rules are lifted in the following three situations:

1. *Anonymization.* When personal data is anonymized, it has become "depersonalized." All identifying details are removed so it can no longer be linked to an individual. Example: Publishing survey results as group statistics without names or contact details. Anonymization must be done carefully to ensure no one can be re-identified even indirectly through unique traits or rare details.
2. *At the individual's request.* A data subject may choose to make their own data public. For example, someone may ask to be listed in a project's directory, or to have their contact information shared in a public report.
3. *Publicly available data sets.* Directories, telephone books, or address books may exist, but only with the written consent of the person whose data is included. Even though such data is not considered confidential, it still requires consent before inclusion.

NOTE FOR CSOS

- √ Never add people to a public list (such as a published report, membership directory, or contact list on your website) without their written consent.
- √ If someone later asks for their data to be removed, you must act promptly.
- √ Even when data is anonymized or made public by consent, ethical handling and respect for people's choices remain essential.

What Other Obligations Do You Have as a Data Controller or Data Processor?

> Articles 17- 21 of the Law on Personal Information
>
> *See also*: Resolution of the Government of the Kyrgyz Republic as of November 21, 2017 N760 on the Approval of the Requirements for Ensuring the Security and Protection of Personal Data during their Processing in Personal Data Information Systems, the Implementation of which Ensures the Established Levels of Protection of Personal Data (Resolution N760).

Being a data controller (the organization that decides why and how personal data is processed) or a data processor (an organization or person who processes data on behalf of the controller) comes with a number of important legal responsibilities under the

law. These duties are meant to protect people's rights and ensure that data is collected, used, and stored responsibly.

Resolution N760 establishes mandatory security requirements for all organizations in Kyrgyzstan that process personal data in information systems, including CSOs. It is based on Article 21 of the Law on Personal Information. It introduces a system of protection levels for personal data and defines what measures organizations must take depending on the level of risk.

There are four levels of data protection, based on the seriousness of threats:

- Blue – minimal risk (basic organizational measures).
- Green – medium risk (requires stronger measures, e.g., encryption).
- Yellow – high risk (requires centralized management, electronic logging, intrusion detection systems).
- Red – critical risk (requires the strictest measures, such as secure communication channels, certified security systems, and annual audits).

CSOs can use the online module developed by the DPA for self-evaluation of the level of risk: https://self-rating.dpa.gov.kg/. Based on the result (blue–red), specific security measures must be implemented.

NOTE FOR CSOS

Resolution N760 sets the standard of care expected for anyone processing personal data in information systems. For CSOs, this means:

- √ Be aware of your level of risk based on the type of data you process. Avoid collecting unnecessary personal data that could raise your risk level (e.g., health information about staff or beneficiaries, which would push you into higher compliance categories).
- √ Implement basic security measures (like policies, responsible staff, access controls, backups, encryption).
- √ If handling sensitive or large volumes of data (e.g., health information, vulnerable groups), consider applying stronger protections.

Do You Need to Register as a Personal Data Holder? How Do You Do It?

> Article 16 and 30 of the Law on Personal Information

Under the Law on Personal Information, any legal entity that works with personal data must first register as a "personal data holder" with the DPA. Without registration, an organization does not have the legal right to process personal data.

If your organization collects or uses personal data (for example, lists of beneficiaries, staff files, volunteer databases, or photos of participants) you are considered a holder of personal data sets and must register with the DPA. The only exception is for data classified as state secrets under the Law on State Secrets, which does not apply to CSOs.

When registering, you must submit detailed information about your data sets, including:

- √ The name of the data set (e.g., "Beneficiary Database").
- √ The organization's details (address, ownership, head of organization, contact details).
- √ The purpose and methods of collecting and using the data.
- √ How long the data will be stored.
- √ The list of personal data you collect (e.g., names, phone numbers, emails).
- √ The categories of people whose data you collect (e.g., beneficiaries, staff, volunteers).
- √ The sources of data (e.g., application forms, surveys).
- √ How individuals are informed about the collection and possible transfer of their data.
- √ Security measures to keep the data safe and confidential.
- √ The person responsible for handling personal data in your CSO.
- √ Any recipients (partners, donors) who may receive the data.
- √ Whether you plan to transfer data abroad.

The DPA maintains a Register of personal data holders. Each year, the DPA publishes this Register in the media, so the public knows which organizations are officially authorized to work with personal data. The registration gives your CSO the legal right to handle personal data and protects your organization against fines for unregistered processing *(please see the section on "What are the penalties for violating personal data laws?" for details)*.

For more information on the registration process, watch the DPA's video guidance here: https://dpa.gov.kg/ru/register/help/5. If you still have questions, contact DPA for consultations and guidance support via WhatsApp at +996 998 950 350.

NOTE FOR CSOS

On July 31, 2025, the President signed the new Digital Code of the Kyrgyz Republic. The Code introduces updated rules for handling personal data and removes the requirement to register as a personal data holder. However, the Code only enters into force six months after its official publication – that is, on February 8, 2026. Importantly, the provisions of the Code on Offenses will come into effect earlier, on November 23, 2025.

This creates a transition period from November 23, 2025, until February 8, 2026, when the DPA may still impose fines for processing personal data without registration, even though the registration requirement will soon be abolished.

During the transition period:

- √ Check if you are registered as a personal data holder with the DPA.
- √ If not yet registered, consider completion of registration before November 23, 2025, to avoid fines.
- √ Maintain compliance with all other data protection requirements (consent, security measures, confidentiality, etc.).
- √ Monitor updates from the DPA on how the registration phase-out will be handled in practice.
- √ Plan ahead: even though registration will no longer be required after February 8, 2026, CSOs must still follow the new Digital Code's rules on handling personal data.

Who Enforces the Law?

> Article 3, 29[1] of the Law on Personal Information
>
> *See also* the Regulation on the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic approved by the Resolution of the Cabinet of Ministers of the Kyrgyz Republic of December 22, 2021, N325.

In Kyrgyzstan, responsibility for enforcing personal data protection rests with the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic (DPA).

The Law on Personal Information, adopted in 2008, set out the basic rules for collecting, processing, and protecting personal data. Before 2021, Kyrgyzstan had a data protection law but no dedicated enforcement body. This meant there was no mechanism for oversight, no procedures to appeal against unlawful actions by data holders, and no sanctions for violations. To ensure data protection rules are implemented and enforced, the government established the DPA in 2021.

The DPA is responsible for ensuring that personal data in Kyrgyzstan is collected, stored, and used lawfully and securely. It monitors compliance with data protection rules, registers organizations as holders of personal data sets, and maintains the official Register. The DPA reviews complaints from citizens, provides guidance to organizations, and can issue binding instructions, warnings, or referrals to law enforcement when violations occur. It also has the authority to demand corrections, blocking, or deletion of inaccurate or unlawfully obtained data. Beyond enforcement, the DPA develops national policy and regulations, drafts standards for safe data handling, cooperates with international data protection authorities, and raises public awareness through reports, training, and research. In short, the DPA both enforces the law and supports organizations in improving their data protection practices.

CONTACT THE DATA PROTECTION AGENCY (DPA)

For official information, tools, and updates: https://dpa.gov.kg

For consultations and guidance support: WhatsApp: +996 998 950 350

What Are the Penalties for Violating Personal Data Laws?

> Code of the Kyrgyz Republic on Offenses
>
> *"Article 413². Violation of Personal Data Protection Requirements*

Article 413² of the Code on Offenses establishes administrative fines for organizations and individuals that fail to follow the legal rules on personal data protection in Kyrgyzstan. This means that if your organization collects, stores, or uses personal data (for example, beneficiary lists, event registrations, or photos of participants), you must comply with the law. If you do not, you risk being fined.

If a CSO mishandles personal data—for example, by collecting it without proper consent, storing it insecurely, or sharing it without authorization—the law provides for the following fines for a first violation:

- Individuals (e.g., staff members): 7,500 KGS
- Officials (e.g., directors, managers): 10,000 KGS
- Legal entities (the CSO itself): 65,000 KGS

If the same violation is repeated within one year after being fined, the penalties increase sharply:

- Individuals: 25,000 KGS
- Officials: 30,000 KGS
- Legal entities: 120,000 KGS

In addition, organizations are fined if they fail to register as a holder of personal data sets. Submitting incomplete or false information to the Register, or processing data without registration, is a violation that carries a fine of 45,000 KGS.

NOTE FOR CSOS

- √ Collect and use personal data lawfully. Always ensure you have consent or another valid legal basis.
- √ Register as a holder of personal data sets if your organization qualifies.
  - Watch the Video Instruction on Completing the Register of Holders of Personal Data Sets.
  - Register through the official website: https://dpa.gov.kg/ru.
- √ Review and update your internal data protection policies to prevent violations. You can use the DPA's Privacy Policy Generator to create a policy for your CSO.
- √ Train your staff on proper handling of personal data. Remember: mistakes by individuals can also result in fines for your organization.

> Code of the Kyrgyz Republic on Offenses
>
> *Article 413³. Cross-Border Transfer of Personal Data in Violation of the Established Procedure*

Many CSOs regularly share data with international donors, partners, or networks. Such activities qualify as "cross-border transfers." Importantly, even using digital tools like Google Forms, Google Drive, or Microsoft OneDrive involves cross-border transfers, since the data is stored on servers outside Kyrgyzstan.

Before transferring data abroad, CSOs must ensure compliance with Kyrgyzstani law. This generally requires either confirmation that the receiving country provides an adequate level of data protection or obtaining the explicit consent of the data subject. *See the section on Cross-Border Transfer of Personal Data above for details on the legal requirements.*

Failure to follow these rules (even unintentionally) can result in significant fines. Under Article 413³, penalties apply when a CSO transfers personal data abroad without meeting the required legal conditions. If a CSO transfers personal data abroad without following the legal procedure (for example, to a country that does not provide adequate data protection), the following fines for the first violation apply:

- Individuals (e.g., staff members): 15,000 KGS
- Officials (e.g., directors, managers): 17,500 KGS
- Legal entities (the CSO itself): 65,000 KGS

If the same violation is repeated within one year after being fined, the penalties increase significantly:

- Individuals: 30,000 KGS
- Officials: 35,000 KGS
- Legal entities: 100,000 KGS

EXAMPLE

BCI collects the names, phone numbers, and email addresses of participants who attend a training. Later, BCI shares the full participant list with an international donor based in Canada by email. Because the donor is based outside Kyrgyzstan, this counts as a cross-border transfer of personal data. If BCI did not obtain the participants' explicit consent for this transfer, or if Canada does not provide adequate data protection, BCI violates Article 413[3]. Even if the transfer was unintentional (for example, a staff member thought it was harmless to send the list), BCI could still face fines.

NOTE FOR CSOS

- √ Always check whether the data you are sharing with international partners includes personal data.
- √ Obtain clear, informed consent from individuals before transferring their data abroad, unless another legal ground applies.
- √ Verify whether the receiving country has adequate legal protections for personal data.
- √ Keep proper documentation—record how consent was obtained and the purpose for the transfer.

> Code of the Kyrgyz Republic on Offenses
>
> *Article 413[4]. Unjustified Refusal by a Holder (Owner) of a Personal Data Set to Provide the Data Subject with Their Personal Data*

Under Kyrgyzstani law, every individual (data subject) has the right to know how their personal data is collected, stored, and used. This means that beneficiaries, staff, or partners may request access to the personal data your organization holds about them (for example, application forms, contact details, or photos). If your organization refuses such a request without a valid legal basis, it will be considered a violation. Importantly, under this Article, only the organization (the legal entity), not individual staff members, can be fined.

- Fine for the first violation: 25,000 KGS

- Fine for a repeat violation within one year: 45,000 KGS

NOTE FOR CSOS

- √ Develop a simple procedure for handling data access requests from beneficiaries, staff, or partners.
- √ Train staff to know when information must be provided and when an exception may apply.
- √ Keep clear records of what personal data your CSO collects and how it is processed. This will make responding to requests easier.
- √ Remember: denying access without a valid legal basis can result in fines for the organization.

> Code of the Kyrgyz Republic on Offenses
>
> *Article 413⁵. Failure to Comply with Lawful Requirements of the Authorized State Body for Personal Data*

The authorized state body for personal data (the State for the Protection of Personal Data under the Cabinet of Ministers or DPA) is responsible for overseeing compliance with personal data protection laws in Kyrgyzstan. It has the legal power to request information, conduct inspections, and issue binding instructions to organizations that process personal data *(see more under the section on "Who enforces the law" of this guidance note)*. For instance, the DPA may require you to fix gaps in your data protection practices, such as registering your personal data sets or updating your privacy policy. Ignoring these instructions or failing to respond on time can result in fines for both individuals and the organization.

If a CSO fails to comply with a lawful request or instruction from DPA, it is considered a violation under Article 413⁵. Fines for non-compliance:

- Individuals (e.g., staff members): 10,000 KGS
- Officials (e.g., directors, managers): 20,000 KGS
- Legal entities (the CSO itself): 30,000 KGS

NOTE FOR CSOS

- √ Always take requests from DPA seriously and respond within the deadlines given.
- √ Keep your records and registration documents organized so they can be provided quickly if requested.

- √ If you are unsure how to comply with a request, seek clarification from DPA in writing.
- √ Remember: both the organization and its managers can be fined for non-compliance.

Relevant Legislation and Regulations

The following normative legal acts were used in preparing this guidance note:

- Law of the Kyrgyz Republic of 14 April 2008 N58 on Personal Information
- Code of Offenses: Articles 413^2–413^5 on personal data violations
- Resolution of the Government of the Kyrgyz Republic of November 21, 2017, N760 on the Approval of the Requirements for Ensuring the Security and Protection of Personal Data during their Processing in Personal Data Information Systems, the Implementation of which Ensures the Established Levels of Protection of Personal Data
- The Regulation on the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic approved by the Resolution of the Cabinet of Ministers of the Kyrgyz Republic of December 22, 2021, N325.
- Order of the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic on the Approval of the Procedure for Obtaining the Consent of a Personal Data Subject for the Collection and Processing of Their Personal Data, including in the Form of an Electronic Document, and for the Purposes of Providing State and Municipal Services dated April 15, 2025, N27
- Order of the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic on the Approval of the Procedure for the Anonymization of Personal Data for the Purposes of Conducting Statistical, Sociological, Historical, Medical, and Other Scientific and Practical Research dated January 14, 2025, N4
- Digital Code of the Kyrgyz Republic adopted on July 31, 2025, entering into force on February 8, 2026