PRIVACY AND PERSONAL DATA PROCESSING POLICY
"Fito centre" Information System and Mobile Application
Effective Date: May 18, 2026
Version: 1.0

This Privacy and Personal Data Processing Policy (hereinafter referred to as the **"Policy"**) is developed in accordance with the legislation of the Republic of Kazakhstan, including Law No. 94-V "On Personal Data and Its Protection" dated May 21, 2013, as well as the requirements of international mobile distribution platforms, Apple App Store and Google Play.

This Policy determines the procedure for the collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer, depersonalization, blocking, and deletion of users' personal data within the framework of the functioning of the **"Fito centre"** information system, web portal, and mobile application (hereinafter jointly referred to as the **"System"**).

1. INFORMATION ABOUT THE SYSTEM OPERATOR (OWNER)

The collection and processing of personal data in the System is carried out by the Owner and Operator of the System:

- **Full Name:** "DRG Systems" Limited Liability Partnership (LLP)
- **Business Identification Number (BIN):** 260240002570
- **Legal Address:** Apartment 39, Building 2/2, Takha Khuseyn St., Baykonyr District, Astana, 010000, Republic of Kazakhstan
- **Contact E-mail:** info@drgsystems.kz
- **Official Website:** drgsystems.kz

2. PURPOSE OF THE SYSTEM AND LEGAL GROUNDS

2.1. The "Fito centre" System is a specialized digital platform intended exclusively for automating phytosanitary monitoring processes, keeping records of phytosanitary objects, conducting field inspections, processing spatial data, and generating official reports (acts).

2.2. The legal grounds for processing personal data are:

- Compliance with the requirements of the legislation of the Republic of Kazakhstan;
- Fulfillment by users of their official, professional, and contractual duties within the framework of phytosanitary control and monitoring;
- Written or electronic consent of the user (including consent certified by an Electronic Digital Signature — EDS).

3. CATEGORIES AND LIST OF PROCESSED DATA

The System processes only the data necessary to perform its target official functions. In accordance with Google Play Data Safety and Apple App Privacy requirements, the collection of the following categories of information is declared:

3.1. User Identification and Registration Data

Data is collected during account registration (which can be created either by the user themselves or centrally by the organization's administrator):

- Full Name (Last Name, First Name, Patronymic);
- Mobile/work phone number;
- E-mail address;
- Individual Identification Number (IIN);
- Job title/Position;
- Name of the organization (employer);
- Details of the legal entity's EDS certificate (during authorization and document signing).

3.2. Geolocation Data (Location Data)

- **Type of Collection:** Precise (GPS) coordinates.

- **Collection Mechanism:** Data is requested and collected **exclusively when opening and actively using the relevant functions** of the application (conducting an inspection, recording a phytosanitary object on the ground).
- **Background Collection:** Continuous background tracking of the user's location (background location) is **not used** in the System.
- **Purpose:** Coordinates are saved on the server to record field work points and correctly display objects on the map.

3.3. Documents, Files, and Media Data

- **Files:** The user has the right to attach and upload documents of various formats (including PDF, Excel, field inspection acts, etc.) to the System's server to perform work tasks.
- **Camera and Photos:** Direct access to the device's camera is not executed. Uploading photo images to the server is not performed (only document files and generated acts are uploaded). The System does not collect or store EXIF metadata of images.

3.4. Technical and Diagnostic Data

When using the System, technical details may be automatically recorded (unique Device IDs, IP addresses, OS types, user action logs and journals) necessary for conducting information security (IS) audits and identifying system errors.

4. AUTHORIZATION AND ACCESS MECHANISMS

4.1. Access to the System is granted to a limited group of people (employees and specialized professionals). There is no public access to the System.

4.2. User authorization in the System is implemented in the following ways:

- Using an e-mail address and password;
- Via the EDS (Electronic Digital Signature) of the National Certification Authority of the Republic of Kazakhstan (only the EDS of a legal entity is accepted).

4.3. The System operates a strict hierarchical role-based access control model, including the roles: Administrator, Inspector, Operator, Manager. All user actions in the System are subject to mandatory internal logging (action journaling).

5. PURPOSES OF DATA PROCESSING

Personal and official data are processed exclusively for the purposes of:

- Ensuring the basic functioning of all System components;
- Identification, authentication, and authorized access of users;
- Documentary registration of phytosanitary inspection results (generation of electronic acts);
- Maintaining security logs and complying with information security requirements (IS audit);
- Ensuring interaction between authorized bodies and specialists within their job descriptions.

6. OFFICIAL OFFLINE MODE (DATA CACHING)

To ensure uninterrupted operation in areas without a stable internet connection, the mobile application features an offline mode. The following may be temporarily cached locally on the user's mobile device:

- Geographic coordinates of inspected points;
- Drafts of acts created during field work.

Upon restoration of the network connection, the data is automatically synchronized with the server part of the System.

7. STORAGE LOCATION, SECURITY, AND DATA PROTECTION

7.1. Server Localization: In accordance with the requirements of the legislation of the Republic of Kazakhstan, the collection and storage of personal data are carried out on servers physically located **within the territory of the Republic of Kazakhstan**. A trusted secure cloud infrastructure is used.

7.2. Protection Measures: Strict organizational and technical measures are applied to ensure the confidentiality and integrity of information:

- Data encryption during transmission using **HTTPS and SSL** protocols;
- Regular data backups to prevent data loss;
- Application of tools to restrict access rights to databases;
- Compliance with information security regulations and conducting IS audits.

8. DATA TRANSFER TO THIRD PARTIES AND INTEGRATIONS

8.1. Third Parties: The Operator **does not transfer**, sell, or disclose users' personal data to commercial third parties.

8.2. State Bodies: Data transfer is permitted exclusively to the state bodies of the Republic of Kazakhstan strictly within the framework of their official duties and authorities established by the legislation of the Republic of Kazakhstan.

8.3. Cross-Border Transfer: The System **does not carry out** the cross-border transfer of personal data (transfer to the territory of foreign states).

8.4. Third-Party Services (Mapping): To visualize spatial data, the System uses external geoinformation and mapping platforms (Google Maps, ArcGIS, OpenStreetMap). Integration with third-party APIs is performed solely to process the map background and spatial coordinates. Third-party services do not have access to users' registration data.

9. DATA AND ACCOUNT DELETION

9.1. Deletion Mechanism: Due to the closed, official nature of the System, for security reasons, the deactivation and complete deletion of a user account (based on an official internal request from an employee or organization) is performed **exclusively by an authorized System Administrator**. Independent account deletion by the user via the mobile app interface is not provided.

9.2. Mandatory Retention: Please note that in accordance with the legislation of the Republic of Kazakhstan and internal regulations of departmental accounting, certain official data (including generated and signed acts of field work, audit journals, and system action logs) **are subject to mandatory archival retention** in the System even after the user's account is deleted.

10. AGE RESTRICTIONS

The System is designed to automate the professional activities of enterprises and government agencies. The product is intended **exclusively for persons of legal age** (over 18 years old) who possess the necessary qualifications. The deliberate collection of data regarding minors is not conducted.

11. NOTIFICATIONS

As part of the performance of official tasks, the System may send users exclusively **service and system push notifications** (regarding the status of act processing, changes in workflows, etc.). The distribution of marketing and advertising materials is not carried out.

12. LANGUAGE VERSIONS OF THE POLICY

This Policy is drafted, approved, and published in the state (**Kazakh**) and **Russian** languages. If necessary to integrate international standards, an English version may be prepared. In the event of discrepancies in the interpretation of the text, the version in the state (Kazakh) language shall prevail.

13. CHANGES AND UPDATES

"DRG Systems" LLP reserves the right to unilaterally update and modify this Policy due to changes in the System's business processes or updates to the legislation of the Republic of Kazakhstan. The new version of the Policy comes into force from the moment it is published on the official website or within the System interface. Users are obliged to independently monitor the relevance of the Policy.

14. CONTACT INFORMATION

For any questions related to the execution of the provisions of this Policy, the withdrawal of consent to data processing, or the clarification of information, you may send a request using the following details:

- **Company Name:** "DRG Systems" LLP
- **E-mail Address:** info@drgsystems.kz
- **Official Website:** drgsystems.kz