NUS WMS Privacy Policy

Edition **v2026-10-23**, in force from **23 October 2026**. This official English version was published on 23 October 2026. Both texts are authentic; in case of any discrepancy between them, the Ukrainian text (https://wms.com.ua/uk/legal/privacy) prevails.

---

1. General provisions

1.1. This Policy explains how BILYI VITER WEB STUDIO LLC (EDRPOU code 40588193, address: 19 Radiievskoho Henerala St., office 215, Kryvyi Rih, Dnipropetrovsk Oblast, 50008, Ukraine; hereinafter the "**Provider**", "**we**") processes personal data as the **controller** (*volodilets* under the PDP Law).

1.2. This Policy applies to the personal data of:

a) visitors to the website https://wms.com.ua (hereinafter the "**Website**"), including with respect to Website analytics to which they have consented (clause 2.1);

b) persons who submit requests through the Website forms or otherwise contact us regarding NUS WMS;

c) representatives and contact persons of Clients — parties to the Agreement concluded under the NUS WMS Public Offer for Residents of Ukraine (https://wms.com.ua/uk/legal/offer-ua) or for Non-residents (https://wms.com.ua/uk/legal/offer-nr) together with the General Terms of Service (https://wms.com.ua/en/legal/general-terms-en) (hereinafter together the "**Offer**");

d) persons who correspond with us, in particular with the support service;

e) Users of the NUS WMS applications — with respect to application usage analytics to which they have consented (clause 2.6), and with respect to the operation of the applications on the device and update checks (clause 2.7).

1.3. This Policy **does not apply** to the personal data that Clients and their Users enter into the NUS WMS Service (Tenant data and User data under clause 10.3 of the General Terms). The Client is the controller of that data, and the Provider is the processor that processes it on the Client's instructions on the terms of Section X of the General Terms. We forward data subjects' requests concerning such data to the relevant Client (clause 10.9 of the General Terms). The exception is application usage analytics (clause 2.6, clause 10.14 of the General Terms): with respect to it, the Provider is the controller.

1.4. We process personal data in accordance with the Law of Ukraine "On Personal Data Protection" (hereinafter the "**PDP Law**") and, where applicable, Regulation (EU) 2016/679 (hereinafter the "**GDPR**").

1.5. The terms "Client", "User", "Service", "applications", "Tenant" and "Demo Environment" are used in the meanings given in the General Terms of Service.

2. What data we process, for what purpose and on what basis

2.1. Website visitors.

- **Data:** IP address; date and time of the request; address of the requested page and of the page from which the visitor came; information about the browser and device (user-agent); server response code — these are recorded by the web server in the server log. The selected interface language — in the `nus.lang` cookie.
- **Purpose:** ensuring the operation and security of the Website, detecting and blocking automated attacks, diagnosing failures; displaying the Website in the selected language.
- **Basis:** the Provider's legitimate interest (item 6 of Part 1 of Article 11 of the PDP Law; Article 6(1)(f) GDPR).

Website analytics — only with consent. If a visitor clicks "Allow" in the cookie notice, the Website uses Google Analytics.

- **Data:** a pseudonymous browser identifier (the `_ga` cookie); pages viewed and actions on them — clicks on request buttons, use of the pricing calculator and the amount it calculates, switching of language and theme, the fact of a form being submitted without its content; date and time; the page or website from which the visitor came and advertising campaign tags (utm); device type, operating system, browser, language, screen resolution; approximate country and city determined from the IP address (Google Analytics does not store the IP address itself).
- **Purpose:** to understand how visitors find and use the Website and to improve it.
- **Basis:** the visitor's consent (item 1 of Part 1 of Article 11 of the PDP Law; Article 6(1)(a) GDPR). Analytics is off until the visitor clicks "Allow"; consent may be withdrawn at any time through the "Cookie settings" link at the bottom of the Website page, after which collection stops. Refusal does not restrict the use of the Website.

Data that a visitor enters into the Website forms is not passed to analytics. We do not create advertising profiles, we have turned off Google Signals and the sharing of analytics data with Google for Google's own purposes, and we do not combine analytics with server logs. There is no advertising and there are no third-party cookies on the Website other than Google Analytics with consent. For more details, see the Cookie Policy (https://wms.com.ua/uk/legal/cookies).

2.2. Persons submitting requests — requests for a demonstration or presentation (including registration for a NUS WMS demonstration), trial requests, partnership requests, and requests by email or phone.

- **Data:** name; phone number; email address; company name; EDRPOU code (for a non-resident — company registration number); line of business or type of enterprise; content of the request; date and time of submission; the IP address and information about the browser and device (user-agent) from which the request was sent, the Website language and the page from which it was sent; advertising campaign tags (utm) of the link through which the visitor came to the Website, and the address of the website from which the visitor came, without its page.
- **Purpose:** responding to the request; conducting a demonstration; assessing the request; providing a trial, in particular checking whether the company has received a trial before; preparing for the conclusion of the Agreement; analysing which channels bring requests.
- **Basis:** the consent that the person gives when submitting the form (item 1 of Part 1 of Article 11 of the PDP Law; Article 6(1)(a) GDPR), and steps taken at the data subject's request prior to entering into a transaction (item 3 of Part 1 of Article 11 of the PDP Law; Article 6(1)(b) GDPR).

The Website adds this information, the advertising campaign tags and the address of the website from which the visitor came to the request itself. If the visitor has clicked "Allow" in the cookie notice, the Website remembers the tags and the address of the website from which the visitor came for the duration of the visit in the `nus.source` cookie (Cookie Policy, https://wms.com.ua/uk/legal/cookies). Without such permission, the Website does not store them: they are carried along in the address of the Website pages the visitor opens, up to the request form.

Requests are registered in our CRM system. To detect repeated requests, we match the EDRPOU code (for a non-resident — company registration number), phone number, email address and company name against existing records.

2.3. Representatives and contact persons of Clients.

- **Data:** surname, first name, patronymic; position; business email address and phone number; the Client's details (for a Client who is an individual entrepreneur, also the data needed for invoices and closing documents); history of invoices and payments.
- **Purpose:** conclusion and performance of the Agreement; keeping records of Clients; Invoices and closing documents; service notifications, in particular about amendments to documents and changes of Subprocessors; compliance with tax and accounting legislation.
- **Basis:** conclusion and performance of a transaction (item 3 of Part 1 of Article 11 of the PDP Law; Article 6(1)(b) GDPR); an obligation provided for by law (item 5 of Part 1 of Article 11 of the PDP Law; Article 6(1)(c) GDPR); legitimate interest — with respect to contact persons of a Client that is a legal entity (item 6 of Part 1 of Article 11 of the PDP Law; Article 6(1)(f) GDPR).

2.4. Correspondence and support requests.

- **Data:** email address, name, content of the message and attachments, date.
- **Purpose:** responding to the request, technical support, handling claims.
- **Basis:** performance of the Agreement — for Clients; legitimate interest — in other cases.

2.5. We do not collect personal data whose processing poses a particular risk (Article 7 of the PDP Law) and ask you not to send such data to us. We do not take decisions producing legal effects for a person based solely on automated processing.

2.6. Application usage analytics.

- **Data:** a pseudonymous identifier of the application instance, generated at installation and not linked to the User's name, login or email address; screen views and use of application features, date and time; application version, operating system and its version, device model, interface language; approximate country determined from the IP address (Google Analytics does not store the IP address itself).
- **Purpose:** improving the Service — understanding which features are used, where Users encounter difficulties, and which platforms and versions need support.
- **Basis:** the User's consent (item 1 of Part 1 of Article 11 of the PDP Law; Article 6(1)(a) GDPR). Analytics is off until the User gives consent in the application; consent may be withdrawn at any time in the application settings, after which collection stops. Refusal does not restrict the use of the Service.

Tenant data (documents, goods, counterparties, etc.) and the names and contact details of Users are not passed to analytics. We do not use device advertising identifiers, do not create advertising profiles, and have turned off the sharing of analytics data with Google for Google's

own purposes.

2.7. NUS WMS applications. This clause describes what the NUS WMS applications for Android, iOS, macOS, Windows and Linux and the web client (https://app.wms.com.ua) do with data on the User's device.

- **Camera.** The Android and iOS applications use the camera only for scanning barcodes and QR codes and only after the permission the User grants in the operating system. The code is recognised on the device; only the value of the code read is transmitted to the Service. Camera images are not stored and are not transmitted anywhere. The permission may be withdrawn in the device settings — camera scanning will then become unavailable, while other functions will keep working. The applications do not request any other permissions giving access to personal data on the device (microphone, location, contacts, photos).
- **Data on the device.** To operate, the application stores on the device: session data — access tokens, the User's email address and name, their role and permissions, the Tenant code; the device identifier (UUID) and the device key (Ed25519) by which the Service recognises a linked device; interface settings (theme, language, list view, scanner parameters); on Android and iOS — a cache of the Tenant's reference data. In the web client, this data is stored in the browser's local storage (localStorage) — see the Cookie Policy (https://wms.com.ua/uk/legal/cookies). On a PDT on which the Client has enabled Offline PDT Mode (clause 3.10 of the General Terms), the Android application additionally stores an encrypted copy of the data of the assigned warehouse (including documents, balances, products and the parties they refer to), the names, badge identifiers and verifiers and a snapshot of the rights of the Users who have access to that warehouse, and a queue of operations not yet transmitted to the Service; the badge secret is not placed on the device in clear. This copy is erased when Offline PDT Mode is disabled or suspended or the device is revoked or blocked (clause 10.15 of the General Terms). This data is deleted together with the application or with the website data in the browser.
- **Data transmitted to the Service.** With each request, the application transmits the device identifier, the platform and the operating mode of the application, and the interface language; when linking a device and signing in — also the application version and the public key of the device; selectively — technical data on request performance; on a PDT with Offline PDT Mode — also operations entered without a connection, with the identifier of the User who entered them, signed with the device key, and confirmation that the local copy has been erased. The application does not transmit the device model, the operating system version or the device name to the Service. The Provider processes this data, like all data that Users enter into Tenants, as a processor on the Client's instructions (clause 10.3 of the General Terms, Section X of the General Terms; clause 1.3 of this Policy).
- **Update checks.** The Android, Windows and macOS applications can check for a new version and download it when the User does so in the application settings. The file with the current version number and the installer are downloaded from Google Cloud Storage; the application transmits no User or device identifiers in doing so, and the versions are compared on the device. Like any web server, Google Cloud Storage receives the IP address and information about the program sending the request (user-agent). The purpose is delivery of updates; the basis is the Provider's legitimate interest in keeping the applications up to date and secure

(item 6 of Part 1 of Article 11 of the PDP Law; Article 6(1)(f) GDPR). We do not link these requests to Users. Applications from the App Store and Google Play may also be updated by means of the store — under its rules.

- **Analytics** — only with the User's consent, see clause 2.6.
- **Advertising and tracking.** The applications do not show advertising, contain no advertising SDKs, do not use device advertising identifiers (IDFA, Android Advertising ID), and do not track Users across other applications and websites.

3. To whom we transfer data

3.1. We do not sell personal data and do not transfer it to third parties for advertising or marketing.

3.2. For processing, we engage service providers acting on our instructions:

Service provider	What it does	Data	Place of processing
Hetzner Online GmbH	Website hosting	Website server logs	EU, Finland
Hetzner Online GmbH	Server of the CRM and the billing system	Requests; data of Clients and contact persons; invoices	EU, Germany
Google Workspace	Corporate email, in particular sending Invoices and closing documents	Correspondence; Invoices and closing documents with the Client's contact details	In accordance with the Google Workspace terms
Google Cloud Platform (Google Cloud Storage)	Distribution of application updates	IP address and user-agent of update download requests (clause 2.7)	EU, Poland
Google LLC (Google Analytics, including Google Analytics for Firebase)	Application and Website usage analytics	Data under clauses 2.1 (Website analytics) and 2.6	USA

3.3. Personal data may be provided to public authorities only in the cases and in the manner provided for by law.

3.4. The List of Subprocessors (https://wms.com.ua/en/legal/subprocessors-en) concerns the Service data that we process as a processor and does not replace the table in clause 3.2.

4. Where data is stored

4.1. The data referred to in this Policy, except application and Website analytics data (clause 4.3), is stored on servers in countries of the European Union — Finland, Germany and Poland, including its backup copies; emails, including Invoices and closing documents, in accordance with the Google Workspace terms.

4.2. The countries of the European Union are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and ensure an adequate level of personal data protection (Article 29 of the PDP Law). Data is transferred to

other third countries only on the basis of the standard contractual clauses applied by the relevant provider.

4.3. Application usage analytics data (clause 2.6) and Website analytics data (clause 2.1) are processed by Google LLC in the USA. The transfer is made on the basis of the consent of the User or the Website visitor (Article 29 of the PDP Law), as well as the EU-US Data Privacy Framework, in which Google LLC participates, and the standard contractual clauses applied by Google.

5. Retention periods

- **Website server logs** — up to 15 days, after which they are automatically destroyed.
- **Requests that did not lead to the conclusion of the Agreement** — 3 years from the last contact with the person or until consent is withdrawn, whichever is earlier.
- **Data of Clients and contact persons** — the term of the Agreement and 3 years after its termination (the general limitation period, Article 257 of the Civil Code of Ukraine); primary documents and invoices — for the periods established by tax and accounting legislation.
- **Correspondence** — 3 years from the date of the last message.
- **Application update download requests** — we do not keep logs of these requests; Google Cloud Storage processes them only to deliver the file.
- **Application usage analytics and Website analytics** — 14 months from the date of the event, after which the data is automatically deleted in Google Analytics; after consent is withdrawn, no new data is collected.
- **Backup copies** of the CRM and the billing system — no longer than one year according to the rotation cycle; data deleted from the system disappears from the backup copies when this cycle is completed.

Upon expiry of the period, the data is destroyed or anonymised.

6. Your rights

6.1. In accordance with Article 8 of the PDP Law and, where applicable, Articles 15–22 GDPR, you have the right:

a) to know who processes your personal data, for what purpose, where it was obtained and where it is processed;

b) to access your personal data;

c) to require the rectification of inaccurate or incomplete data;

d) to require the erasure of data or the restriction of its processing;

e) to object to processing carried out on the basis of legitimate interest;

f) to receive your data in a structured, machine-readable format — if the GDPR applies;

g) to withdraw consent at any time; the withdrawal does not affect the lawfulness of processing before it;

h) to lodge a complaint with the Ukrainian Parliament Commissioner for Human Rights or with a court and, if the GDPR applies, also with the supervisory authority of the EU Member State of your habitual residence or place of work.

6.2. Send your request to support@wms.com.ua with the subject "Personal data". We may ask you to confirm that the request is being sent by you. We respond within 30 calendar days from the date of receipt of the request.

7. Security

7.1. We apply organisational and technical protection measures: encryption of connections (HTTPS / TLS), access control based on the principle of least privilege, multi-factor authentication for administrative access, and backups.

7.2. Only employees who need access to personal data to perform their duties and who are bound to keep it confidential have such access.

8. Children

The Website and the Service are intended for businesses and are not addressed to persons under 18 years of age. We do not knowingly collect their personal data.

9. Amendments to the Policy

9.1. Amendments are made by a new edition of the Policy stating its effective date. The current edition is available at https://wms.com.ua/en/legal/privacy-en, all previous ones — in the Archive of editions (https://wms.com.ua/uk/legal/archive).

9.2. If a new edition provides for processing for new purposes requiring consent, we will ask for such consent separately.

10. Contacts

BILYI VITER WEB STUDIO LIMITED LIABILITY COMPANY

- EDRPOU code: 40588193
- Address: 19 Radiievskoho Henerala St., office 215, Kryvyi Rih, Dnipropetrovsk Oblast, 50008, Ukraine
- Email: support@wms.com.ua
- Phone: +380 63 616-09-22, +380 98 616-09-22

End of edition v2026-10-23.