# YES PDF

## GDPR Compliance Report

**EU GENERAL DATA PROTECTION REGULATION (EU) 2016/679**

Software Version: 1.1.2

Document Version: 1.0

Date: February 2026

Classification: Public

# YES BILISIM

YES BILISIM TEKNOLOJILERI YAZILIM DANISMANLIK SAN. VE TIC. A.S.

https://yespdf.com.tr

# Table of Contents

**1. Executive Summary**

**2. Product Overview**

**3. Roles & Responsibilities** — Data Controller, Processor, Software Provider

**4. Data Collected by the Vendor** — License & customer information only

**5. Data Processed On-Premise** — User accounts, documents, audit logs

**6. Optional External Integrations** — DeepL, Email, LDAP/AD

**7. Security Measures** — Encryption, authentication, access control

**8. Data Subject Rights (GDPR Art. 15-22)**

**9. Data Retention & Deletion**

**10. Data Sharing & Transfers**

**11. Compliance Statement**

# 1. Executive Summary

Yes PDF is an **on-premise** enterprise PDF management platform. It is installed and operated entirely within the customer's own infrastructure. No end-user data is collected, transmitted to, or accessible by the software vendor (Yes Bilisim).

**Yes PDF is designed for GDPR compliance by architecture.**
All personal data processing occurs exclusively on the customer's own servers.
The vendor holds zero end-user data.

This report documents:

- What data is processed by Yes PDF and where it resides
- The roles and responsibilities of the vendor and the customer
- Technical and organizational security measures implemented
- How GDPR data subject rights are supported
- Data retention and deletion policies

> **Vendor Data Footprint:** The only information held by Yes Bilisim (the vendor) is the **customer company name** and a **machine signature** (SHA-256 hash of hardware identifiers) for license binding. No personally identifiable information (PII) of end users is collected or processed by the vendor.

# 2. Product Overview

| Attribute | Details |
|---|---|
| **Product Name** | Yes PDF |
| **Current Version** | 1.1.2 |
| **Deployment Model** | On-Premise (customer-hosted) |
| **Architecture** | Web-based application (FastAPI backend, browser frontend) |
| **Database** | PostgreSQL 16 or SQLite (customer-managed) |
| **Operating System** | Windows Server 2016+ / Windows 10+ |

| | |
|---|---|
| **Network** | Runs on local network; no internet connection required for core features |
| **Vendor** | Yes Bilisim Teknolojileri Yazilim Danismanlik San. ve Tic. A.S. |

Yes PDF provides centralized PDF viewing, editing, conversion, OCR, digital workflow tools, and document management through a web browser. All processing is performed locally on the customer's server.

# 3. Roles & Responsibilities

## 3.1 Definitions under GDPR

| Role | Entity | Explanation |
|---|---|---|
| **Data Controller**<br>**GDPR Art. 4(7)** | The Customer Organization | The customer determines the purposes and means of processing personal data within the Yes PDF installation. They decide which users to create, what documents to process, and how long to retain data. |
| **Data Processor**<br>**GDPR Art. 4(8)** | **Not Applicable** | Yes Bilisim does NOT process personal data on behalf of the customer. The software runs entirely on the customer's infrastructure with no data transmitted to the vendor. Yes Bilisim is a software provider, not a data processor. |
| **Software Provider** | Yes Bilisim | Yes Bilisim provides the Yes PDF software, installation support, and license management. The vendor has no access to the customer's Yes PDF installation, user data, or documents. |

**Key Distinction:** Because Yes PDF is an on-premise product with no data transmission to the vendor, no Data Processing Agreement (DPA) between the vendor and customer is required under GDPR. The customer is the sole Data Controller for all personal data within their installation.

## 3.2 Customer Responsibilities

As the Data Controller, the customer organization is responsible for:

- Ensuring lawful basis for processing personal data within Yes PDF
- Managing user accounts and access permissions
- Configuring data retention policies appropriately
- Responding to data subject access requests (DSARs)

- Maintaining physical and network security of the server hosting Yes PDF
- Evaluating optional external integrations (DeepL, SMTP, LDAP) for their own GDPR compliance

# 4. Data Collected by the Vendor

Yes Bilisim collects the absolute minimum data required for software licensing:

| Data Item | Purpose | PII? | Retention |
|---|---|---|---|
| **Customer / Company Name** | License issuance and identification | No (company name) | Duration of license |
| **Customer Contact Email** | License delivery and support communication | Typically business email | Duration of license |
| **Machine Signature** | License binding to specific server | No (SHA-256 hash) | Duration of license |

## 4.1 Machine Signature Details

The machine signature is a **one-way SHA-256 hash** generated from hardware identifiers (hostname, architecture, disk serial, motherboard serial, MAC address). It is:

- **Non-reversible** — the original hardware details cannot be extracted from the hash
- **Non-personal** — identifies a server, not a person
- **Format**: `XXXX-XXXX-XXXX-XXXX` (16 hex characters)

## 4.2 What the Vendor Does NOT Collect

> **The vendor does NOT collect:**
>
> - End-user names, email addresses, or passwords
> - Documents or document metadata
> - Usage statistics, telemetry, or analytics
> - Crash reports or diagnostic data
> - IP addresses or browsing behavior
> - Any data from the customer's Yes PDF installation

Yes PDF contains **no telemetry, no analytics, no phone-home functionality, and no automatic update checks**. The software makes zero outbound network connections to the vendor.

# 5. Data Processed On-Premise

The following data is processed and stored entirely within the customer's infrastructure. The vendor has no access to this data.

## 5.1 User Accounts

| Data Field | Type | Purpose | Protection |
|---|---|---|---|
| Email address | String | Authentication, identification | Database access control |
| Display name | String | UI display | Database access control |
| Password | Hash | Authentication | bcrypt one-way hash (never plain text) |
| Role | Enum | Authorization (admin/user) | Database access control |
| Account status | Boolean | Enable/disable access | Database access control |
| Login timestamp | DateTime | Audit trail | Database access control |
| LDAP DN / GUID | String | Directory sync (if LDAP enabled) | Database access control |

## 5.2 Documents

| Data Field | Protection |
|---|---|
| PDF files | **AES-256-CBC encryption at rest** with per-installation key and per-file random salt |
| Original filename | Database access control |
| File metadata (size, page count) | Database access control |
| OCR extracted text | Database access control |

> **Encryption Details:** All stored PDF files are encrypted using AES-256-CBC with PBKDF2-SHA256 key derivation (100,000 iterations). Each file has a unique 16-byte random salt and 16-byte random initialization vector. The encryption key is auto-generated per installation and stored in the server's environment configuration.

## 5.3 Audit Logs

Yes PDF maintains comprehensive audit logs for security and compliance purposes:

- **Logged actions:** Login/logout, document upload/download/delete, PDF operations, admin actions
- **Logged context:** User email, action type, IP address, user agent, timestamp
- **Default retention:** 365 days (configurable by the customer)
- **Storage:** Database table + rotating log files (20-day file rotation)

## 5.4 Sessions

- Stored **server-side only** (not in client cookies or local storage)
- Contains: session ID, user ID, email, IP address, user agent
- Maximum lifetime: 24 hours (configurable)
- Idle timeout: 60 minutes (configurable)
- Automatic cleanup of expired sessions every 5 minutes
- Single session per user enforced (prevents concurrent sessions)

# 6. Optional External Integrations

Yes PDF supports optional integrations that may involve external data transfer. All integrations are **disabled by default** and must be explicitly configured by the customer.

> **Important:** When enabling external integrations, the customer (as Data Controller) is responsible for evaluating the GDPR compliance of the third-party service and obtaining any necessary consent or legal basis.

## 6.1 DeepL Translation API

| Attribute | Details |
|---|---|
| **Status** | Disabled by default; requires customer-provided API key |
| **Data sent to DeepL** | Document text content for translation, source/target language |
| **Data received** | Translated text, detected language |
| **DeepL GDPR status** | DeepL SE is an EU company (Cologne, Germany) with GDPR compliance |
| **Customer action** | Review DeepL's privacy policy before enabling; consider DPA with DeepL if translating documents containing personal data |

## 6.2 IMAP / SMTP Email

| Attribute | Details |
|---|---|
| **Status** | Disabled by default; requires customer email server configuration |
| **Data processed** | Sender email address, email subject, PDF attachments |
| **Data flow** | Customer's email server → Yes PDF (local) → auto-reply via SMTP |
| **Storage** | Email credentials stored in local database (never transmitted to vendor) |

| | |
|---|---|
| **Customer action** | Ensure email server complies with organizational data policies |

## 6.3 LDAP / Active Directory

| Attribute | Details |
|---|---|
| **Status** | Disabled by default; requires customer AD server configuration |
| **Data synced** | User email, display name, DN, GUID, group membership (read-only) |
| **Data flow** | Customer's Active Directory → Yes PDF (local) |
| **Direction** | One-way: AD → Yes PDF (Yes PDF never writes back to AD) |
| **Customer action** | Standard internal system; typically covered by employee data processing policies |

# 7. Security Measures

Yes PDF implements comprehensive technical and organizational security measures in accordance with **GDPR Art. 32** (Security of Processing).

## 7.1 Data Encryption

| Layer | Method | Details |
|---|---|---|
| Files at Rest | AES-256-CBC | Per-installation key, per-file random salt (16 bytes), per-file random IV (16 bytes), PBKDF2-SHA256 100K iterations |
| Passwords | bcrypt | One-way hash; never stored or logged in plain text |
| Session IDs | SHA-256 | 32 cryptographically random bytes hashed |
| Secret Keys | Auto-generated | SECRET_KEY and ENCRYPTION_KEY auto-generated on first startup |
| Network (optional) | TLS/SSL | HTTPS support; HSTS header enabled (1 year) |
| Database (PostgreSQL) | SCRAM-SHA-256 | pg_hba.conf hardened to reject weaker auth |

## 7.2 Access Control

- **Role-based access**: Admin and User roles with strict permission boundaries
- **Per-user document isolation**: Users can only access their own documents
- **Admin IP restriction**: Optional whitelist for admin panel access
- **Forced password change**: Required on first login
- **Password policy**: Minimum 12 characters, uppercase, lowercase, digit, special character required
- **Single session enforcement**: One active session per user

## 7.3 Attack Prevention

| Threat | Mitigation |
|---|---|

| | |
|---|---|
| Brute Force | Rate limiting: 5 login attempts per 5 minutes, 15-minute lockout |
| XSS | Global `escapeHtml()` sanitization on all user-generated content in templates |
| CSRF | Double-submit cookie pattern on all state-changing requests |
| SQL Injection | Parameterized queries (SQLAlchemy ORM) + middleware detection |
| Clickjacking | X-Frame-Options: DENY |
| MIME Sniffing | X-Content-Type-Options: nosniff |
| Information Leakage | Referrer-Policy: strict-origin-when-cross-origin |

**Security Audit:** Yes PDF v1.1.1 underwent a comprehensive security audit with 28 of 30 findings remediated, including 6 critical-severity items. See the Release History for details.

## 8. Data Subject Rights (GDPR Articles 15-22)

Yes PDF provides administrative tools that enable the customer (Data Controller) to fulfill data subject requests:

| Right | GDPR Article | Yes PDF Support |
|---|---|---|
| **Right of Access** | **Art. 15** | Admin panel displays all user data (profile, documents, audit history). Data can be exported for the data subject. |
| **Right to Rectification** | **Art. 16** | Admin can update user email, name, and all profile fields. Users can update their own profile. |
| **Right to Erasure** | **Art. 17** | Admin can delete a user account, which cascade-deletes all associated data (documents, audit entries, job records). |
| **Right to Restriction** | **Art. 18** | Admin can disable a user account (is_active = false), preventing all access without deleting data. |
| **Right to Data Portability** | **Art. 20** | Users can download all their documents. Admin can export user profile data. |
| **Right to Object** | **Art. 21** | Not applicable — Yes PDF performs no profiling, automated decision-making, or direct marketing. |
| **Automated Decision-Making** | **Art. 22** | Not applicable — Yes PDF makes no automated decisions with legal effects on individuals. |

> **Implementation Note:** The customer (Data Controller) is responsible for establishing procedures to receive, verify, and respond to data subject requests within the GDPR-mandated 30-day timeframe. Yes PDF provides the technical tools to fulfill these requests.

# 9. Data Retention & Deletion

Yes PDF implements configurable data retention policies. The customer can adjust these settings to match their organizational requirements.

| Data Type | Default Retention | Configurable? | Deletion Method |
|---|---|---|---|
| User Accounts | Until manually deleted | N/A | Admin delete (cascade deletes all related data) |
| Documents | Until manually deleted | N/A | User or admin delete |
| Audit Logs (DB) | 365 days | Yes (`AUDIT_LOG_RETENTION_DAYS`) | Automatic purge after retention period |
| Log Files | 20 days | Yes | Daily rotation with automatic deletion |
| Job Queue Records | 7 days | Yes (`QUEUE_CLEANUP_DAYS`) | Automatic cleanup |
| Sessions | 24 hours / 60 min idle | Yes | Automatic expiry + cleanup every 5 minutes |

## 9.1 Uninstall Behavior

- **Application files:** Removed on uninstall
- **User documents (uploads folder):** Preserved on uninstall to prevent accidental data loss
- **Database:** Preserved on uninstall (customer must manually delete if desired)
- **Log files:** Removed with application

# 10. Data Sharing & Transfers

## 10.1 No Data Sharing with Vendor

Yes PDF transmits **zero data** to the vendor (Yes Bilisim).
There is no telemetry, analytics, crash reporting, usage tracking, or automatic update mechanism.

## 10.2 No Third-Party Data Sharing

Yes PDF does not share, sell, or transmit user data to any third party. The only external data flows are the optional integrations described in Section 6, which are:

- Disabled by default
- Explicitly configured by the customer
- Under the customer's control and responsibility

## 10.3 International Data Transfers

As an on-premise product, Yes PDF does not transfer data internationally. Data resides exclusively on the customer's server in the customer's chosen jurisdiction.

If the customer enables the DeepL integration, text data may be sent to DeepL SE servers in Germany (EU). This is subject to DeepL's own GDPR compliance and the customer's assessment.

## 10.4 Sub-Processors

Yes Bilisim employs **no sub-processors** for the Yes PDF product. All software components are bundled locally:

- PDF processing: Apryse SDK (bundled, runs locally)
- OCR engine: Tesseract (bundled, runs locally)
- Database: PostgreSQL (bundled, runs locally)
- Web server: FastAPI/Uvicorn (bundled, runs locally)

# 11. Compliance Statement

**GDPR Compliance by Design & Default (Art. 25)**

Yes PDF is architected with privacy by design and by default:

- **Data Minimization:** Only essential data is collected (user email, name for authentication)
- **Storage Limitation:** Configurable retention periods with automatic cleanup
- **Integrity & Confidentiality:** AES-256 encryption at rest, bcrypt password hashing, comprehensive security controls
- **Purpose Limitation:** All data is processed solely for the purpose of providing PDF management functionality
- **Transparency:** Complete audit logging of all data operations
- **Data Sovereignty:** On-premise deployment ensures the customer retains full control over all data

Yes PDF enables organizations to process PDF documents in a GDPR-compliant manner by keeping all personal data within the customer's own infrastructure, implementing strong security controls, and providing administrative tools for data subject rights fulfillment.

---

| Document Information | |
|---|---|
| Document Title | Yes PDF GDPR Compliance Report |
| Version | 1.0 |
| Date | February 2026 |
| Software Version | 1.1.2 |
| Author | Yes Bilisim Teknolojileri |

| | |
|---|---|
| Classification | Public |
| Next Review | February 2027 |