

Ringkasan Keamanan & Privasi Data Arkantara

Oktober 2026 · Arkantara

Ringkasan

Data setiap sekolah disimpan terpisah, hanya dapat dibuka oleh pengguna yang berhak, dan setiap perubahan penting tercatat. Dokumen ini menjelaskan cara Arkantara menjaga data siswa, wali, dan pegawai, serta hal yang tetap menjadi tanggung jawab sekolah.

- Data tiap sekolah berada di skema basis data sendiri; berkasnya di ruang penyimpanan terpisah per sekolah.
- Masuk dilindungi kata sandi ber-hash, verifikasi dua langkah, passkey, dan pembatasan percobaan.
- Hak akses diatur per peran; admin sekolah tidak dapat memberi hak melebihi haknya sendiri.
- Log audit tidak dapat diubah atau dihapus, kecuali oleh proses retensi setelah 730 hari.
- Basis data dicadangkan setiap hari ke penyimpanan terpisah.
- Sekolah dapat mengekspor seluruh datanya kapan saja.

Dokumen ini mengikuti Kebijakan Privasi Arkantara yang berlaku sejak 23 Oktober 2026; bila ada perbedaan, Kebijakan Privasi yang berlaku.

Peran sekolah dan peran Arkantara

Sekolah adalah pengendali data pribadi atas data yang dikelolanya; CV Bulung Gadung, operator Arkantara, adalah prosesor yang memproses data itu hanya untuk menjalankan layanan sesuai perjanjian dan instruksi sekolah. Istilah ini mengikuti UU 27/2022 tentang Pelindungan Data Pribadi.

Hal	Sekolah	Arkantara
Data yang dicatat	Menentukan data siswa, wali, pegawai, nilai, keuangan, dan dokumen yang diisi	Menyediakan aplikasi dan menyimpan data sesuai pilihan sekolah
Dasar pemrosesan data anak	Memastikan dasar yang sah, termasuk persetujuan orang tua atau wali bila diperlukan	Tidak memakai data anak untuk iklan, pemasaran, atau profil di luar keperluan sekolah
Siapa yang boleh mengakses	Memberi peran dan mencabut akses pengguna	Menegakkan hak akses dan mencatat perubahannya
Permintaan dari siswa atau wali	Menjawab permintaan akses, koreksi, dan penghapusan	Membantu sekolah dengan fitur ekspor, ubah, dan arsip
Data platform sendiri	—	Pengendali atas kontak tagihan sekolah, akun pengelola, permintaan demo, catatan dukungan, dan log keamanan

Kontrol keamanan di produk

Semua kontrol berikut berjalan di setiap paket, kecuali yang ditandai Enterprise.

Kontrol	Cara kerjanya
Pemisahan data	Setiap sekolah punya skema basis data sendiri dan ruang berkas sendiri; satu akun hanya terhubung ke satu sekolah.
Koneksi	Seluruh koneksi memakai HTTPS dengan HSTS.
Kata sandi	Disimpan sebagai hash, bukan teks aslinya; mengganti kata sandi mengeluarkan perangkat lain.
Verifikasi dua langkah	Kode aplikasi autentikator dengan sepuluh kode cadangan; wajib bagi pengelola platform, tersedia bagi semua pengguna sekolah.
Passkey	Masuk dengan sidik jari, wajah, PIN perangkat, atau kunci keamanan, terikat ke alamat sekolah.
Perlindungan formulir	Percobaan masuk dibatasi per IP dan email; formulir masuk, daftar, reset sandi, dan formulir publik memakai verifikasi anti-bot Cloudflare Turnstile.
Hak akses	Peran bawaan dan peran buatan sekolah; admin tidak dapat memberi hak melebihi haknya sendiri; modul di luar paket tertutup; orang tua hanya melihat anak yang ditautkan.
Berkas	Hanya dapat diunduh setelah izin diperiksa, lewat tautan sementara 60 detik; jenis dan isi berkas divalidasi; metadata foto, termasuk lokasi, dibuang.
Rahasia	Kunci verifikasi dua langkah, kredensial pembayaran DOKU sekolah, dan kunci API email disimpan terenkripsi.
Log audit	Perubahan penting dicatat dengan pelaku, waktu, dan nilai sebelum/sesudah; log tidak dapat diubah atau dihapus. Tampilan log lengkap untuk sekolah: Enterprise.
Sesi	Setiap pengguna melihat dan mencabut sesinya sendiri; riwayat masuk dan sesi seluruh sekolah: Enterprise.
Akses dukungan	Pengelola platform hanya dapat masuk sebagai pengguna sekolah dengan konfirmasi kata sandi, alasan, dan verifikasi anti-bot; paling lama 30 menit; setiap tindakan tercatat.
Dokumen tercetak	Rapor, surat, surat kelulusan, sertifikat, dan kuitansi memuat QR verifikasi yang hanya menampilkan nama tersamar, tanpa nilai.

Penyimpanan, backup, dan retensi

Berkas dan backup disimpan di Cloudflare R2, yang mengenkripsi setiap objek dengan AES-256; basis data dicadangkan setiap hari dan salinannya disimpan 31 hari.

Data	Lama disimpan
Data operasional sekolah	Selama sekolah memakai Arkantara; sekolah mengarsipkan atau menghapus lewat fitur yang tersedia
Backup basis data	Dibuat setiap hari, disalin ke bucket R2 terpisah, dikunci 30 hari, lalu dihapus otomatis setelah 31 hari
Log audit	730 hari
Notifikasi yang sudah dibaca	180 hari

Data	Lama disimpan
Pesan chat yang dihapus pengirimnya	Dihapus permanen setelah 365 hari
Dokumen yang diarsipkan beserta berkasnya	1.825 hari setelah diarsipkan
Berkas ekspor data sekolah	7 hari setelah dibuat
Akun daftar sendiri yang tidak dikonfirmasi	Dinonaktifkan setelah 24 jam dan emailnya dilepas

Setelah berhenti berlangganan, data sekolah tetap tersimpan dan dapat diekspor selama sekolah belum diarsipkan atau ditangguhkan. Atas permintaan sekolah, data dapat dikosongkan permanen paling cepat 30 hari setelah sekolah diarsipkan: akun dianonimkan, basis data sekolah dikosongkan, dan berkasnya dihapus. Catatan langganan, tagihan, log audit, dan riwayat dukungan tetap disimpan untuk keperluan hukum dan pembukuan.

Penyedia pihak ketiga

Setiap penyedia hanya menerima data yang diperlukan untuk fungsinya; sebagian dapat memproses data di luar Indonesia.

Penyedia	Fungsi	Data yang diterima
Cloudflare	Jaringan dan perlindungan lalu lintas, penyimpanan berkas privat dan backup (R2), verifikasi anti-bot Turnstile, domain kustom sekolah	Lalu lintas situs, berkas, token verifikasi dan alamat IP
Resend	Pengiriman email	Alamat penerima, subjek, dan isi email
DOKU	Pembayaran daring bila diaktifkan sekolah, dan tagihan langganan	Jumlah dan nomor tagihan, nama dan ID siswa atau sekolah, email pembayar; data kartu dan rekening tidak melewati Arkantara
Google	Masuk dengan akun Google, bila pengguna memilihnya	Alamat email dan ID akun Google
Layanan notifikasi peramban	Notifikasi perangkat, bila pengguna mengaktifkannya	Isi notifikasi terenkripsi
Sentry	Pelaporan galat aplikasi, bila diaktifkan	Konteks teknis galat; email, IP, cookie, dan isi permintaan dibuang
Penyedia pusat data	Server aplikasi dan basis data	Data aplikasi yang dijalankan di server

Hak sekolah dan penanganan insiden

Data tetap milik sekolah: sekolah dapat mengekspor seluruhnya kapan saja dan meminta penghapusan permanen setelah berhenti.

- **Ekspor data.** Admin sekolah membuat satu berkas ZIP berisi CSV per tabel dan seluruh berkas unggahan dari menu Pengaturan > Ekspor data. Kata sandi, kredensial pembayaran, dan pesan langsung antarpengguna tidak ikut. Berkas dapat diunduh 7 hari, dan setiap permintaan tercatat.
- **Koreksi dan penghapusan.** Pengguna yang berhak mengubah, mengarsipkan, atau menghapus data lewat fitur di aplikasi; perubahan tercatat di log audit.
- **Permintaan subjek data.** Siswa, wali, dan pegawai mengajukan permintaan tentang datanya lebih dulu ke sekolah; Arkantara membantu sekolah memenuhinya.
- **Insiden.** Bila terjadi kegagalan perlindungan data pribadi, Arkantara memberi tahu sekolah yang terdampak tanpa penundaan. Untuk data yang dikendalikan Arkantara sendiri, Arkantara memberi tahu subjek data dan lembaga yang berwenang sesuai UU PDP.
- **Kontak privasi.** privasi@arkantara.com.

Batas yang perlu diketahui

Kontrol di atas adalah kontrol teknis; Arkantara belum memiliki sertifikasi keamanan pihak ketiga.

- Belum ada audit atau sertifikasi independen (misalnya ISO 27001) dan belum ada uji penetrasi pihak ketiga.
- Kunci enkripsi penyimpanan R2 dikelola Cloudflare, bukan oleh sekolah.
- Sebagian penyedia dapat memproses data di luar Indonesia.
- Keamanan juga bergantung pada sekolah: mengaktifkan verifikasi dua langkah bagi admin, mencabut akses pegawai yang keluar, dan tidak membagikan akun.
- Pemantauan perilaku saat ujian CBT bersifat pencegahan; keputusan tetap di tangan pengawas.

Sumber dan dokumen terkait

- [Kebijakan Privasi Arkantara](#), berlaku sejak 23 Oktober 2026
- [Syarat Layanan Arkantara](#)
- [Cloudflare R2: keamanan data](#) (enkripsi AES-256 saat disimpan, TLS saat transit)
- [Hukumonline: program perlindungan data pribadi](#) (kewajiban pencatatan pemrosesan, Pasal 31 UU PDP)