Teknik ve idari tedbirler

12 Kasım 2026 tarihli sürüm · Bilgi amaçlı çeviridir. Bağlayıcı olan Almanca metindir.

Ön not

Önlemler, Alman veri koruma denetim makamlarının Standart Veri Koruma Modeli'nin koruma hedeflerine göre yapılandırılmıştır. SchuleVernetzt, SavePaperwork tarafından tek kişilik bir işletme olarak geliştirilir ve işletilir.

1. Veri minimizasyonu

- Öğrencilerin hesabı yoktur. Yalnızca adları, soyadları ve sınıfları tutulur; doğum tarihi, adres, telefon numarası ve fotoğraf yoktur.
- Hastalık gerekçesi yalnızca okul bunu açarsa sorulur; soru varsayılan olarak kapalıdır. Öğretmenlerin devamsızlık bildirimlerinde gerekçe hiçbir zaman saklanmaz.
- Okullar doktor raporu yüklemeyi kapatabilir; Kuzey Ren-Vestfalya, Brandenburg ve Berlin'deki okullar için bu özellik varsayılan olarak kapalıdır.
- Bildirimler mümkün olduğunca az bilgi içerir: bir mesaj bildirimi yalnızca göndereni belirtir, konuyu veya metni belirtmez; kilit ekranındaki bir doktor raporu hatırlatması hiçbir çocuğu belirtmez.
- Okul işletmecisi (Schulträger) hesabı yalnızca okul adlarını ve temel rakamları görür, kişileri görmez.
- Sınıf bağlantısı ve fuaye ekranı öğrenci adlarını ve devamsız öğretmenleri göstermez.
- Okul yönetimi onayladıktan sonra, veri türü başına eyaletin sürelerine göre silme.
- Denetim kaydındaki okuma erişimi kayıtları (yanıtlanmış erişim taleplerinin kanıtları hariç) 90 gün sonra, uygulama günlükleri 14 gün sonra silinir; okulun denetim kaydı IP adreslerini saklamaz.
- Barındırma sağlayıcısı, arızaları incelemek ve kötüye kullanımı önlemek için erişim kayıtlarını tam IP adresiyle 90 güne kadar, hata kayıtlarını 7 güne kadar saklar.
- Okulun sayfalarında ve okulun e-postalarında hiçbir analiz veya takip hizmeti ve hiçbir üçüncü taraf yazı tipi çalışmaz.

2. Erişilebilirlik

- Frankfurt am Main'da ISO 27001 sertifikalı bir veri merkezinde işletim (barındırma sağlayıcısının beyanına göre).
- Barındırma sağlayıcısı tarafından günlük yedekleme; AES-256 ile şifreli, Helsinki'deki ayrı bir veri merkezinde, 90 gün saklanır.
- Yeni sürümlere atomik olarak geçilir; önceki sürüme her zaman geri dönülebilir. Veri tabanı şemasındaki değişiklikler hiçbir zaman otomatik uygulanmaz.
- İşletmecinin telefonuna uyarılarla birlikte, her beş dakikada bir otomatik izleme (veri tabanı, arka plan işleri, hata yığılmaları).
- Ağ kesintisi sırasında da sınıf defteri tutulmaya devam edilebilir; kayıtlar, cihaz yeniden çevrimiçi olur olmaz gönderilir.
- Okul, sözleşme sona erdikten sonra bile her zaman tüm verilerin eksiksiz bir dışa aktarımını kendisi indirebilir (dışa aktarma garantisi).
- Hedef, duyurulan bakımlar hariç, yıllık ortalama olarak %99,5 erişilebilirliktir.

3. Bütünlük

- Şifreli içerik, kimliği doğrulanmış şifreleme kullanır; her değişiklik okuma sırasında tespit edilir ve sessizce kabul edilmez.
- Denetim kaydı, bir kaydı kimin, ne zaman oluşturduğunu, değiştirdiğini veya sildiğini eski ve yeni değerle birlikte kaydeder; hassas değerler bu kayıtta karartılır.
- Formlar siteler arası istek sahteciliğine karşı korunur; girdiler sunucuda doğrulanır.

- Yüklenen dosyaların türü ve içeriği kontrol edilir (PDF, JPG, PNG, WebP, DOCX; en fazla 10 MB; çift uzantı yok) ve rastgele bir adla saklanır.
- Koddaki her değişiklik, okullar arasındaki ayrımın testleri de dahil olmak üzere otomatik testlerden geçer.

4. Gizlilik

- Roller ve yetkiler: okul yönetimi her şeyi görür; okul sekreterliği yalnızca kendisine açıkça serbest bırakılanı; öğretmenler yalnızca kendi sınıflarını ve derslerini; veliler yalnızca kendi çocuklarını. Hastalık gerekçesini yalnızca okul yönetimi, okul sekreterliği ve sınıf öğretmeni okuyabilir ve ona yapılan her okuma erişimi kaydedilir.
- Okulların ayrılması: tüm veriler tam olarak tek bir okula aittir; her sorgu o okulla sınırlıdır.
- Hastalık gerekçeleri, not değerleri ve yorumları, karne metinleri, öğrencilere ilişkin sınıf defteri kayıtları, mesajlar ve yüklenen tüm dosyalar için uygulamada şifreleme (libsodium; alanlar için XSalsa20-Poly1305, dosyalar için XChaCha20-Poly1305). Anahtar yalnızca sunucu yapılandırmasında tutulur; dosya depolama sağlayıcısı yalnızca şifreli veriyi alır.
- İletim yalnızca HSTS ile HTTPS üzerinden; oturum çerezleri yalnızca HTTPS üzerinden ve betikler tarafından okunamaz.
- Okulun alanlarında bir Content Security Policy yalnızca platformun kendi betiklerine izin verir; tarayıcı enjekte edilen kodu çalıştırmaz ve başka hiçbir site bu alanları gömemez.
- Parolalar yalnızca karma değeri olarak (bcrypt veya Argon2); parola değiştirildiğinde oturumlar sonlandırılır; parola sıfırlama bağlantıları 24 saat geçerlidir ve yalnızca bir kez kullanılabilir.
- Tahmin saldırılarına karşı koruma: art arda en fazla beş oturum açma denemesi ve ayrıca üçüncü taraf sağlayıcı olmadan bir hesaplama bulmacası (ALTCHA).
- Okul sekreterliği ve okul işletmecisi için zorunlu, okul yönetimi için kullanılabilir ikinci faktör (TOTP) ve ayrıca geçiş anahtarları (passkey). Öğretmenler ve veliler de ikinci faktörü açabilir; okul bunu öğretmen kadrosu için zorunlu kılabilir. Okullar okul girişini (OIDC, örneğin Microsoft Entra, Google veya bir eyalet girişi) kurabilir ve onun çok faktörlü kimlik doğrulamasını kullanabilir.
- Dosyalar, herkese açık erişimi olmayan özel depolamada tutulur ve yalnızca yetki kontrolünden sonra uygulama üzerinden teslim edilir.
- Uygulama günlüklerini yalnızca işletmeci okuyabilir; bir filtre, herhangi bir şey yazılmadan önce adresleri, parametreleri, sırları ve belirteçleri kaldırır.
- Sunucunun erişim bilgileri yalnızca korumalı bir yapılandırma dosyasında tutulur; geliştirme ve test ortamları üretim depolamasına erişemez.
- İşletmeci, bir okulun verilerine yalnızca işletim, arıza giderme veya okuldan gelen bir talep gerektirdiğinde erişir; işletmeci, § 203 StGB (Alman Ceza Kanunu) uyarınca gizlilikle bağlıdır. Bunun için “Kullanıcı değiştir” işleviyle okuldan bir kişi olarak oturum açarsa, eylemleri okulun denetim kaydında o kişinin eylemleri olarak değil, adıyla birlikte “İşletmeci (SavePaperwork)” olarak görünür.

5. Bağlantısızlık (amaçla sınırlama)

- Veriler yalnızca okul için işlenir: reklam yok, profilleme yok, ifşa yok, yapay zekâ modellerinin eğitilmesi yok; okul ürününe hiçbir yapay zekâ hizmeti entegre edilmemiştir.
- Bir okul ağı, her okul katılıp her alan için (vekil havuzu, kurslar, materyaller) onay verene kadar hiçbir şey paylaşmaz; talep eden okul, bir vekil öğretmenin iletişim bilgilerini ancak serbest bırakıldıktan sonra görür. Ağdan ayrılmak erişimi derhal keser.
- Okulların üretim verileri hiçbir zaman geliştirme veya test ortamlarına kopyalanmaz; orada işletmeci kurgusal örnek verilerle çalışır.

6. Şeffaflık

- Okul yönetimi, denetim kaydında hangi verileri kimin değiştirdiğini ve hassas veri içeren hangi listeleri kimin açtığını görür.

- Sözleşme, önlemler, alt işleyenler, eyaletlere göre saklama süreleri, etki değerlendirmesi ve işleme faaliyetleri kaydı için şablonlar ile veliler, personel ve öğrenciler için bilgilendirme metinleri herkese açıktır.
- Yeni alt işleyenler 30 gün önceden duyurulur.

7. Müdahale edilebilirlik

- Bilgi alma ve veri taşınabilirliği: bir öğrencinin veya velinin tüm verilerinin tek tıkla dışa aktarılması; tüm okulun her zaman dışa aktarılması.
- Düzeltme, silme ve kısıtlamayı okul uygulamada kendisi yapar.
- Saklama sürelerini, alanları, hastalık gerekçesi sorusunu ve velilere görünürlüğü okul kendisi belirler; bir sınıf bağlantısı istenildiği zaman yenilenebilir veya kapatılabilir.
- Veri ihlallerinin okula gecikmeden, kural olarak 24 saat içinde bildirilmesi.

8. Organizasyon

- SavePaperwork tek kişilik bir işletmedir; sahibi platformu bizzat geliştirir ve işletir. Başka kişilere erişim, yalnızca gizlilik ve § 203 StGB ile bağlandıktan sonra verilir.
- Yeni sürümleri yalnızca sahibi, sunucuyla kendi şifreli bağlantısı üzerinden dağıtır.
- Şu anda bir veri koruma görevlisi atanmamıştır; irtibat kişisi sahibidir.
- Bu önlemler, platformdaki her önemli değişiklikte ve en az yılda bir gözden geçirilir.