Documento provisional (borrador) — Esta plantilla sirve como base de discusión. El documento definitivo lo revisa nuestro asesor legal antes de ser firmado con cualquier cliente. Si necesitas el DPA finalizado para firmarlo, contáctanos en info@vigilatum.es.

Acuerdo de Encargado del Tratamiento (DPA) — PLANTILLA

⚠️ **BORRADOR — NO es asesoramiento legal.** Esta plantilla la debe revisar y adaptar un abogado antes de firmarla con ningún cliente. Cubre los puntos que el RGPD (UE) 2016/679 exige en el art. 28 para un encargado del tratamiento. Vigilatum captura **telemetría de red y, opcionalmente, capturas de tráfico (pcap)** → hay datos potencialmente personales, así que este DPA es obligatorio incluso en beta gratuito.

1. Partes y roles

- **Responsable del tratamiento (Controller):** el CLIENTE (la empresa monitorizada).
- **Encargado del tratamiento (Processor):** Vigilatum (tú / tu sociedad).
- Vigilatum trata datos **únicamente por instrucción del Cliente** y para prestar el servicio de monitorización.

2. Objeto, duración, naturaleza y finalidad

- **Objeto:** monitorización de red y diagnóstico de incidencias del Cliente.
- **Finalidad:** detectar caídas/degradaciones, diagnosticar causa raíz, y (si está activado) capturar evidencia forense de red durante incidencias.
- **Duración:** mientras dure el contrato de servicio; al terminar, se borran los datos (cláusula 9).

3. Categorías de datos tratados

- **Telemetría de red:** RTT, pérdida, jitter, estado DNS/HTTP, métricas de sistema (CPU/RAM/disco), inventario IoT/LAN (MAC, IP, vendor, hostname).
- **Perfil WAN:** IP pública, ISP/ASN, geolocalización aproximada de la sede.
- **Capturas de tráfico (pcap) — SOLO si el módulo forensic está activado:** paquetes de red de la sede durante ventanas de incidencia. **Pueden contener datos personales** (IPs internas, metadatos, y según el tráfico, payload). Por eso la retención es mínima (24h) y el acceso restringido.

- **NO se tratan** categorías especiales (art. 9 RGPD) de forma intencionada. El Cliente debe valorar si su tráfico capturado puede contenerlas.

4. Categorías de interesados

Empleados del Cliente y cualquier usuario de su red cuya actividad genere tráfico monitorizado.

5. Ubicación del tratamiento y subencargados

- **Hosting:** Hetzner Online GmbH — centro de datos en **Núremberg, Alemania (UE)**. Datos **dentro del EEE** → sin transferencias internacionales.
- **Subencargados autorizados:** | Subencargado | Servicio | Ubicación | |---|---|---| | Hetzner Online GmbH | Hosting / infraestructura | Alemania (UE) | | (correo: ip-api.com) | Geolocalización IP del perfil WAN | revisar ubicación/base legal |
- Vigilatum notificará al Cliente cualquier cambio de subencargado con antelación razonable.

> NOTA: revisa la base legal de **ip-api.com** (geolocalización). Si no quieres dependencia externa, considera geolocalización local o eliminar el campo geo del wan_profile.

6. Medidas técnicas y organizativas (art. 32)

- **Cifrado en tránsito:** TLS en todas las comunicaciones; **mTLS** (certificado mutuo) para la autenticación de sondas.
- **Sonda solo saliente:** la sonda NUNCA acepta conexiones entrantes; solo hace llamadas HTTPS salientes. Vigilatum no se conecta a la red del Cliente.
- **Aislamiento multi-tenant:** datos segregados por `tenant_id`, verificado por tests automatizados.
- **Control de acceso:** autenticación JWT, separación de roles operador/cliente, gate de aprobación manual de sondas.
- **Minimización y retención:** métricas 90 días; capturas pcap/bundles forenses **borrados a las 24h**.
- **Auditoría:** registro de remediaciones y accesos.

7. Confidencialidad

El personal de Vigilatum con acceso a datos está sujeto a deber de confidencialidad.

8. Asistencia al Responsable

Vigilatum asistirá al Cliente, en la medida razonable, en: respuesta a derechos de los interesados (acceso, supresión…), evaluaciones de impacto (DPIA) y notificación de brechas.

9. Supresión al finalizar

Al terminar el contrato, Vigilatum borrará o devolverá todos los datos del Cliente en un plazo de [30] días, salvo obligación legal de conservación.

10. Notificación de brechas

Vigilatum notificará al Cliente sin dilación indebida (objetivo: **< 48-72h**) tras tener conocimiento de una brecha de seguridad que afecte a sus datos.

11. Auditoría

El Cliente podrá auditar el cumplimiento (o recibir evidencia documental) una vez al año con preaviso razonable.

Checklist antes de firmar con el primer cliente

- [ ] Abogado revisa y adapta esta plantilla.
- [ ] Decidir base legal de ip-api.com o eliminar geo.
- [ ] Publicar Política de Privacidad (ver `PRIVACY_RETENTION.md`).
- [ ] Tener un proceso real de notificación de brechas (a quién, cómo, en cuánto).
- [ ] Confirmar el DPA de Hetzner como subencargado (Hetzner ofrece su propio AVV/DPA).
