

Vertragsposition: Managed Disclosure für betriebene Kundenauftritte

ENTWURF - noch nicht abschließend; einzelne Stellen sind zu ergänzen. Diese Position ergänzt den Auftragsverarbeitungsvertrag und den zugrunde liegenden Betriebsvertrag. Sie ist nicht rechtsverbindlich, solange sie nicht als verbindliche Fassung veröffentlicht ist.

Stand: v1-2026-08

1. Warum es diese Position gibt

Gosign betreibt einen öffentlichen Meldeweg für Sicherheitslücken. Betrifft eine Meldung einen von Gosign betriebenen Kundenauftritt, handelt Gosign dafür als **Auftragsverarbeiter**: Verantwortlicher ist der Kunde, und er entscheidet über die Behebung. Das ist keine Formalie — es bestimmt, was Gosign einem Melder überhaupt zusagen kann.

Diese Position schreibt auf, was Gosign beim Meldeweg leistet, was ausdrücklich nicht, und wie der Kunde die Zusage an Meldende übertragen kann, damit sie auch auf seinem Auftritt gilt.

2. Geschuldete Leistung

Leistung	Inhalt
Annahme	Gosign nimmt Meldungen über das eigene Meldeformular entgegen, vergibt eine Vorgangsnummer und bestätigt dem Melder den Eingang. Der Vorgang wird gespeichert, bevor irgendetwas anderes geschieht.
Weiterleitung	Gosign leitet die Meldung unverzüglich an die vom Kunden benannte Empfängeradresse weiter. Bestehen Anhaltspunkte für einen Zugriff auf personenbezogene Daten , geschieht das ohne Zwischenschritt: Die gesetzliche Frist des Kunden beginnt mit seiner Kenntnis, und die darf Gosign nicht verzögern.
Nachweis der Übergabe	Gosign hält Zeitpunkt, Empfänger und Zustellstatus jeder Weiterleitung fest und legt diesen Nachweis dem Kunden auf Anforderung vor. Reagiert der Kunde nicht, weist Gosign ihn schriftlich auf das Risiko hin.

3. Nicht geschuldete Leistung

Die häufigste Falscherwartung an einen Meldeweg ist Erkennung. Deshalb steht hier, was Gosign aus dieser Position **nicht** schuldet:

- Gosign **sucht keine Schwachstellen** im Auftritt des Kunden — weder anlassbezogen noch fortlaufend. - Gosign **bewertet** eine gemeldete Lücke **nicht** abschließend auf Richtigkeit, Schweregrad oder Ausnutzbarkeit; eine erste Einschätzung ist eine Serviceleistung, keine Zusicherung. - Gosign **behebt** die gemeldete Lücke **nicht** aus dieser Position. Eine Behebung ist Gegenstand des Betriebs- oder Wartungsvertrags und wird gesondert beauftragt. - Gosign **überwacht** den Auftritt **nicht** auf Angriffe, Ausnutzung oder Wiederauftreten. - Gosign zahlt **keine Prämien** und betreibt kein Bug-Bounty-Programm. Das gilt auch für Meldungen zu Kundenauftritten.

4. Mitwirkung des Kunden und Rechtsfolge

Der Kunde benennt eine **Empfängeradresse** für Sicherheitsmeldungen und hält sie aktuell. Er benennt eine Vertretung für Abwesenheiten. [VON LEGAL/OPS ZU ERGÄNZEN: Frist, innerhalb derer eine Änderung mitzuteilen ist]

Rechtsfolge. Ist die benannte Adresse nicht erreichbar oder nicht aktuell, **ruht** die Weiterleitungszusage aus Ziffer 2, solange dieser Zustand andauert. Gosign nimmt Meldungen weiter an und dokumentiert den Zustellversuch; die Zusage einer unverzüglichen Übergabe kann Gosign ohne erreichbaren Empfänger nicht halten. Die gesetzlichen Pflichten des Kunden bleiben davon unberührt — sie treffen ihn unabhängig davon, ob ihn die Meldung erreicht hat.

5. Übertragung der Zusage an Meldende

Auf der Policy-Seite sagt Gosign gutgläubig Meldenden zu, auf Strafantrag und auf zivilrechtliche Ansprüche zu verzichten. **Für den Auftritt des Kunden kann Gosign diese Zusage nicht aus eigenem Recht geben** — über dessen Systeme und Daten verfügt Gosign nicht, und auf fremde Rechte kann niemand verzichten.

Mit dieser Ziffer **überträgt** der Kunde die Zusage auf seinen Auftritt:

Der Kunde verzichtet gegenüber Personen, die eine Schwachstelle **gutgläubig** und unter Einhaltung der nachstehenden Grenzen melden, auf einen **Strafantrag** sowie auf **zivilrechtliche** Ansprüche wegen des Auffindens und der Meldung der Schwachstelle.

Die Zusage gilt nur innerhalb derselben Grenzen wie auf der Policy-Seite. Sie entfällt, wenn der Meldende:

- auf **fremde Daten** zugreift, sie kopiert, verändert oder löscht, statt den Zugriff nur nachzuweisen, - die **Verfügbarkeit** oder Integrität des Systems beeinträchtigt, etwa durch Lasttests oder Manipulation des Betriebs, - die Schwachstelle vor ihrer Behebung **weitergibt** oder veröffentlicht, außerhalb der auf der Policy-Seite genannten Frist.

Wirkung nach außen. Hat der Kunde die Zusage übertragen, wird das in der security.txt seines Auftritts ausgewiesen und nennt ihn namentlich — nur so kann ein Melder erkennen, dass sie von demjenigen stammt, der sie geben kann. Ohne Übertragung schweigt die Datei dazu: Gosign nimmt Meldungen entgegen, leitet sie weiter und setzt sich beim Betreiber ein, sagt darüber hinaus für diesen Auftritt aber nichts zu.

[VON LEGAL/OPS ZU ERGÄNZEN: ob die Übertragung mit dem Betriebsvertrag endet oder für bis dahin erfolgte Meldungen fortwirkt]

6. Verhältnis zu den übrigen Vereinbarungen

Diese Position ergänzt den Auftragsverarbeitungsvertrag und den Betriebsvertrag; bei Widersprüchen in datenschutzrechtlichen Fragen geht der Auftragsverarbeitungsvertrag vor. Die öffentliche Policy-Seite bindet Gosign gegenüber dem Melder — diese Position sagt dem Kunden gegenüber nichts zu, was ihr widerspricht.

ENTWURF - noch nicht abschließend. Vor der Freigabe werden die mit ERGÄNZEN gekennzeichneten Stellen gefüllt. Stand: **v1-2026-08**.