1 Security

Signhost is a market leader in the field of electronic signatures and electronic identification. Ondertekenen.nl and Signhost.com are solutions that are supplied by Signhost. The security of information is imperative to Signhost. We make every conceivable effort to prevent unauthorised access to our clients' confidential information, to ensure that the information is correct and available whenever required. That is why Signhost takes a proactive approach to secure its systems and keep all information safe.

The method that is used for electronic signatures must be reliable and secure. We guard the quality and reliability of our services 24/7. The security of our services satisfies the industry's most stringent standards at every level. We are the partner you can trust when it comes to having documents, such as PDF files, signed electronically. Furthermore, Signhost ensures that its procedures and processes are drawn up and designed in accordance with commonly accepted standards (good practices), such as ISO 27001 and COBIT. **Signhost' Certifications and Accreditations**

Signhost holds the following certifications and accreditations:

- ISO/IEC 27001: 2013 certification
- Service Organization Control (SOC) 2 Type 2 – statement
- DigiD TPM statement
- iDIN – Digital Identity Service Provider (DISP)

Signhost wants to be able to demonstrate to customers that it has its information security in order. That is why we have been complying with the requirements of ISO/IEC 27001 since March 2017: the 'de facto' standard for information security.

Click here for the certificate.

1.1 SOC2 TYPE 2

Signhost is compliant to the SOC 2 Type 2 requirements. This statement garantuees customers the high service level of product development and Signhost.com. SOC 2 Type 2 refers to the infrastructure, software, procedures, people and data of an online service provider and what requirements are needed to meet the highest international standards. Hereby both foreign as domestic organisations know what to expect.

1.2 THIRD-PARTY STATEMENT (TPM) FOR DIGID

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Logius requires an annual report on the ICT security assessment of DigiD. That audit is conducted by a registered EDP auditor (RE auditor) of an independent certified party, which will draw up a Third-Party Statement (TPM) following the audit.

Signhost issues the TPM to its clients who use DigiD every year.

1.3 IDIN – DIGITAL IDENTITY SERVICE PROVIDER (DISP)

Signhost is Digital Identity Service Provider (DISP) for iDIN. The Dutch Payments Association has officially certified Signhost to help companies use iDIN on their own website. As a DISP, Signhost is allowed to provide iDIN services directly to “acceptors” without the intervention of a bank. These can be web shops or government services that use iDIN to identify a user or to allow a customer to log in.

1.4 HOSTINGPROVIDER

Signhost operates in a secure data centre in the Netherlands. This data centre also meets the requirements of ISO/IEC 27001:2022 and NEN 7510:2011.

1.5 HOSTINGPROVIDER

Every year, our hosting provider issues an ISAE 3402 Type II accreditation to provide insight into the reliability of its services.

1.6 COORDINATED VULNERABILITY DISCLOSURE

Signhost has guidelines for reporting vulnerabilities, which helps us to protect our systems and clients. Should you discover any specific security issues, please let us know as soon as possible so that we can take immediate action.

1.7 DATA-ENCRYPTION

All connections to the Signhost web application or connections made via an API link travel through a secure SSL connection. The technology behind an SSL connection ensures that data are encrypted; it is also used for Internet banking.

1.8 SECURE DATA CENTRE

Signhost operates in a secure data centre in the Netherlands. Our secure-hosting partner meets the ISO 27001 information security standard. Our hosting provider also has ISAE3402 Type II Assurance accreditation.

1.9 LEGALLY VALID

Signhost meets the requirements for advanced electronic signatures as laid down in Section 3:15(a) of the Dutch Civil Code and the eIDAS Regulation. See our explanation of legal validity.

1.10 ROUND-THE-CLOCK MONITORING

Internal and external tools are used to ensure round-the-clock protection of the Signhost service against vulnerabilities. We use the OWASP guidelines to detect any security issues.

1.11 PENETRATION TESTS

At least once a year, Signhost's web environments are subjected to penetration tests as part of the ICT security assessment for DigiD in line with the NOREA 'DigiD Assessments Manual V2.0'. These penetration tests are carried out by multiple external parties on a rotating basis.

1.12 PRIVACY STATEMENT

In our privacy and cookie statement we explain, among other things, which of your personal data we collect and the purposes for which they are collected. We also use this statement to provide information on the cookies that are installed. We attach great importance to providing you with information on these subjects in a clear and transparent way. Please do not hesitate to contact us if you have any questions about the processing of your personal data or about this statement.

1.13 PROCESSING AGREEMENT

It is important that agreements concerning the processing of personal data are laid down by contract to remain in line with current and future privacy legislation. As an additional service, Signhost provides all its clients with a standard processing agreement to ensure that both parties act in accordance with privacy legislation. This processing agreement takes account of the requirements that arise from the General Data Protection Regulation.

1.14 CONTINGENCY PLAN FOR DATA LEAKS

We believe it is important not only to enter into contractual agreements with you on reporting data leaks, but also to ensure that these agreements are honoured. That is why we have developed internal processes that enable us to identify and follow up on data leaks in good time. Signhost has a contingency plan for data leaks that describes how we deal with any such leaks. You may inspect the contingency plan upon request.

1.15 PERSONAL DATA SECURITY

In accordance with Section 13 of the Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens) and with the General Data Protection Regulation, as from 25 May 2018, Signhost has taken appropriate technical and organisational measures to protect personal data against loss and unlawful processing. Signhost also takes account of the policy rules of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), such as the 'Policy rules on the security of personal data (2013)'.

1.16 GENERAL DATA PROTECTION REGULATION (GDPR)

As from 25 May 2018, the Dutch Data Protection Act has been replaced by the GDPR. The GDPR entails additional obligations for organisations, such as keeping a processing register, honouring additional rights of data subjects and, in certain cases, conducting mandatory data protection impact assessments. Signhost is aware of these changes and has ensured that it has been acting in accordance with the GDPR since 25 May 2018.